Date de réception : 23/01/2015

11

COURT OF JUSTICE OF THE EUROPEAN UNION

Preliminary Reference in Case C-362/14

Between:-

MAXIMILLIAN SCHREMS

Applicant

-and-

DATA PROTECTION COMMISSIONER

Respondent

OUTLINE WRITTEN SUBMISSIONS OF THE DATA PROTECTION COMMISSIONER

CONTENTS

A) INTRODUCTION

Background to the judicial review that led to this request for a preliminary ruling

1) Facebook Ireland Limited is a limited liability having its registered office at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

2) All subscribers to the *Facebook* social media platform who are resident in the European Union / European Economic Area are required to enter into contract with Facebook Ireland Limited.

3) On 25 June 2013[1], the Applicant made a complaint to the Data Protection Commissioner ("**the DP Commissioner**") alleging that:

   (i) Facebook Ireland Limited was transferring personal data relating to Facebook subscribers resident in the EU/EEA to servers located in the United States, owned or controlled by its parent company, Facebook Inc.; and,

   (ii) Facebook Inc. was in turn providing the United States National Security Agency with direct and unhindered access to bulk data held on its servers, including data relating to Facebook subscribers resident in the EU/EEA.

4) The Applicant's complaint was based on the revelations made by Edward Snowden to the effect that the National Security Agency had established a programme (referred to as the "PRISM" programme) under which it obtained unhindered access to bulk data held on servers located in the United States, owned and/or controlled, not just by the operators of the *Facebook* social media platform, but by a range of different internet and technology companies, including Apple, Skype, Microsoft, and others.

5) The DP Commissioner formed the opinion that the Applicant's complaint should not be admitted to investigation as the complaint was bound to fail. As such, it was properly to be considered "frivolous or vexatious" within the narrow, technical meaning of those

[1] See Attachment 1

words as used in Section 10(1)(b)(i) of the DP Acts. The DP Commissioner formed that opinion in light of the following:

(i) Section 11 of the Data Protection Acts 1988-2003[2] ("**the DP Acts**");

(ii) Commission Decision No. C2000/520/EC[3] ("**the Commission Decision**");

(iii) the terms of the Safe Harbour Privacy Principles and FAQs; and,

(iv) Facebook's self-certified adherence to the Safe Harbour Principles and FAQs[4] (such certification having been verified by the DP Commissioner's office by examining entries noted on a publicly-accessible register operated by the United States Department of Commerce).

6) In the judicial review that has led to this request for a preliminary ruling the Applicant seeks to quash the opinion formed by the DP Commissioner that his complaint should not be admitted to investigation. It is to be noted that the Applicant did not bring any challenge to the validity of the 1995 Directive or the Commission Decision in his proceedings.

7) The desired outcome that the Applicant sought from his proceedings before the Irish courts is apparent from his letter of complaint dated 25 June 2013 in which he sought the following of the DP Commissioner:

(i) That the DP Commissioner review the validity of the Commission Decision, which in turn incorporates the Safe Harbour Privacy Principles and FAQs;

(ii) If necessary, that the DP Commissioner obtain a preliminary ruling from the CJEU on the validity of the Commission Decision; and,

(iii) If necessary, that the DP Commissioner prohibit the transfer of personal data by Facebook Ireland Limited to Facebook Inc. unless Facebook Ireland

[2] See Attachment 2

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=EN

[4] http://safeharbor.export.gov/companyinfo.aspx?id=23019

Limited could disprove reports of the "PRISM" programme.

The nature of the question raised before this Court

8) The question raised before this Court is essentially a jurisdictional question, namely, whether it was open to the DP Commissioner to challenge the Safe Harbour Principles and FAQ on the grounds advanced by the Applicant, in circumstances where the DP Commissioner is bound by the terms of the Commission Decision.

9) The DP Commissioner submits that he acted within jurisdiction in declining to investigate the complaint in circumstances where:

   i) The Commission Decision represents a "Community Finding" within the meaning of that term as set out in Section 11(2)(a) of the DP Acts, which in turn follows the provisions of Article 25(6) of the Directive 95/46/EC[5] ("**the 1995 Directive**");

   ii) Under Section 11 of the DP Acts, the DP Commissioner is bound to apply that Community Finding; and,

   iii) The Applicant did not allege that there was a substantial likelihood that the Safe Harbour Privacy Principles and FAQ are being violated by Facebook Ireland Limited and/or Facebook Inc. Nor did he provide evidence of any such violation. Accordingly, the complaint made did not engage Article 3 of the Commission Decision. On the contrary, the Applicant sought to challenge the terms of the Safe Harbour regime itself on the grounds that there is no meaningful protection in United States' law and practice in respect of data transferred to the United States, so far as State surveillance is concerned.

10) In these circumstances, it is submitted that the actions of the DP Commissioner demonstrated scrupulous adherence to the application of the law as he understands it to

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&qid=1414083125498&from=EN

be, represented by the 1995 Directive and the terms of the Commission Decision.

11) As regards the substantive question of whether a National Data Protection Authority can and/or should look behind a Community Finding in order to preserve the rights of individuals (and the particular circumstances in which that approach might be taken), it is submitted that any substantive discussion of these issues is properly a matter for the EU Commission and the Member States themselves.

12) The DP Commissioner acknowledges that this referral raises important and complex legal issues regarding how, and by whom, the rights of individuals are to be vindicated in this rapidly developing area. The DP Commissioner welcomes the clarity that will be brought to these issues by this referral.

13) It is emphasized that, in the proceedings before the Irish High Court, the Applicant chose not to bring any challenge to the validity of the 1995 Directive or the Commission Decision. Rather his challenge was limited to the opinion formed by the DP Commissioner that the Applicant's complaint should not be admitted to investigation for the reasons outlined (in summary terms) at paragraph 5 above.

B) NATURE OF OPINION FORMED BY THE DP COMMISSIONER

14) As noted above, the proceedings before the Irish High Court arose from a challenge to the fact that DP Commissioner declined to investigate the complaint having formed the opinion that it was unsustainable in law or, to use the language of Section 10(1)(b)(i) of the DP Acts, the complaint was "frivolous or vexatious".

15) In ***Nowak v Data Protection Commissioner***[6] the Irish High Court (Birmingham J) explained the nature of such an opinion formed under Section 10(1)(b)(i) in the following terms:

> *"Once the Commissioner had formed the view that the examination script did not constitute personal data it followed that he was being asked to proceed with*

[6] [2013] 1 ILRM 207; see Attachment 3.

an investigation where no breach of the Data Protection Acts could be identified. It was in those circumstances he had resort to s. 10(1)(b)(i). That section refers to complaints that are frivolous or vexatious. However, I do not understand these terms to be necessarily pejorative. Frivolous, in this context does not mean only foolish or silly, but rather a complaint that was futile, or misconceived or hopeless in the sense that it was incapable of achieving the desired outcome..." (page 216)(emphasis added).

16) Similarly, in the judgment delivered in these proceedings in the Irish High Court, Hogan J made the following observations (at paragraph 39 of his judgment[7]) on the meaning of the words "frivolous and vexatious" as used in the particular context of Section 10(1)(b)(i) of the DP Acts:

> *"It is certainly true that in the ordinary sense of these words the present complaint – raising as it does weighty issues of transcendent importance in relation to data protection – is neither "frivolous" nor "vexatious". While in this respect the actual language of s.10(1)(b) of the 1988 Act is somewhat unfortunate and perhaps even unhelpful, nevertheless, as Birmingham J. pointed out in Novak, in this particular statutory context these words also apply to a case where the claim is considered to be unsustainable in law."*

17) It is also relevant to note that the forming of an opinion by the DP Commissioner at a particular point in time that a particular complaint is not admissible is not necessarily a final one for all time. Nor does it preclude a fresh complaint being made if the law changes or if further evidence becomes available. For example, if the Commission Decision were to be revoked and/or replaced at some future date then clearly any new complaint that the Applicant might wish to bring would fall to be considered under the new legal regime in place. However the DP Commissioner has to have regard to the state of the law as it stands at the time when he is considering a particular complaint. That is what was done in this case.

[7] [2014] IEHC 310; see Attachment 4.

C) THE RELEVANT LEGAL FRAMEWORK

Domestic law

18) Ireland has implemented its obligations as regards data protection into domestic law by means of the DP Acts. The DP Commissioner is established pursuant to those Acts and is bound by them in terms of the scope of his powers.

19) Section 10(1) of the DP Acts provides for the power to investigate complaints and states that:

> (a) The DP Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.
>
> (b) Where a complaint is made to the DP Commissioner under paragraph (a) of this subsection, the DP Commissioner shall-
>
> (i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious, and,
>
> (ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it to the Court under section 26 of this Act within 21 days from the receipt by him or her of the notification.

In this case the DP Commissioner formed the opinion that the Applicant's complaint was "frivolous or vexatious" in the sense that it was bound to fail for the reasons summarized at paragraph 5 above. On that basis, he declined to investigate the

complaint.

20) Section 11 of the DP Acts addresses the issue of the transfer of personal data outside of the State. Section 11(2)(a), which was inserted by the Data Protection (Amendment) Act, 2003, provides that the DP Commissioner is bound by a Community Finding:

> (a) Where in any proceedings under this Act a question arises-
>
> (i) whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area to which personal data are to be transferred, and
>
> (ii) a Community finding has been made in relation to transfers of the kind in question,
>
> the question shall be determined in accordance with that finding.

21) Section 11(2)(b) of the DP Acts defines the concept of a Community finding in the following terms:

> *"In paragraph (a) of this subsection 'Community finding' means a finding of the European Commission made for the purposes of paragraph (4) or (6) of Article 25 of the Directive under the procedure provided for in Article 31(2) of the Directive in relation to whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area."*

22) The Commission Decision is made pursuant to Article 25(6) of the 1995 Directive and so comes within the definition of a 'Community finding'.

23) Section 11(2) of the DP Acts makes it clear that where matters relating to international data transfer out of the EU have been dealt with at an EU level then it is not for domestic regulators to seek to go behind that. One can readily see the logic of this since

it would be very difficult for the EU to trade with the United States if every Member State took a different approach to this issue. It is the type of issue that is more appropriately dealt with at an inter-governmental level with the involvement of bodies such as the Commission and the Parliament.

24) There are also practical difficulties which arise out of a domestic regulator seeking to engage with political, diplomatic and trade issues. It is also difficult to see how a single domestic regulator can police what does or does not happen in the United States. The DP Commissioner's powers under the DP Acts are not extra-territorial.

EU law

25) The DP Acts were enacted to give effect to the Data Protection Convention 1981[8] and the 1995 Directive.

26) Article 16 of the Treaty on the Functioning of the European Union[9] also makes express reference to the need to protect personal data and provides that "Everyone has the right to protection of personal data concerning him or her." Article 8(1) of the Charter of Fundamental Rights of the European Union[10] is expressed in precisely the same terms. The Charter goes on to provide as follows at Articles 8(2) and 8(3):

> "2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which had been collected concerning him or her, and the right to have it rectified.*
>
> 3. *Compliance with these rules shall be subject to control by an independent authority."*

[8] http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[9] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=en

[10] http://www.europarl.europa.eu/charter/pdf/text_en.pdf

27) In respect of some countries (such as Argentina, Canada, Israel and Switzerland) the Commission has issued individual decisions recognising them as providing adequate protection for personal data on the basis that those countries have generally applicable data protection laws which follow the approach of the Directive.

28) The Commission Decision was adopted to establish the Safe Harbour Principles and FAQs as a reference point for permissible data transfers to the United States on the basis that the United States has a different approach to data protection than the EU (being based on piece-meal legislation, self-regulation and consumer action). The Safe Harbour regime was introduced against the backdrop of concerns that personal data would stop flowing to the United States after the implementation of the 1995 Directive in the EU.[11] The Safe Harbour Privacy Principles and FAQs were issued by the United States Department of Commerce on 21 July 2000 and, following the adoption of the Commission Decision on 26 July 2000, they came into effect in November 2000.

29) The Commission Decision is thus the relevant 'Community finding' that governs this area of the law and, as such, the DP Commissioner is bound to take notice of it and to apply it.

30) Participation by individual organisations in the Safe Harbour framework is voluntary. Where an organisation elects to participate, however, it is required to certify to the United States Department of Commerce that it is operating in compliance with the Safe Harbour Privacy Principles and FAQs. Amongst other things, it must adopt a publicly stated privacy policy incorporating the standards set out in the Privacy Principles and the FAQs. Upon so certifying, the Privacy Principles and FAQs become legally binding on the organisation in question and they may be enforced against it. Certification remains in force for a period of 12 months following which it may be renewed. The organisation must make an annual return to the Department of Commerce confirming its continued compliance.

[11] See generally Jay, *Data Protection Law and Practice* (Sweet and Maxwell, 4th ed. 2012), Chapter 8; see Attachment 5.

31) Participants in the framework are required to adopt effective and independent complaints and dispute resolution procedures. Separately, and depending on the particular sector in which they operate, they must subject themselves to regulation by the Federal Trade Commission or the United States' Department of Transportation.

32) The United States' Department of Commerce maintains a publicly accessible list[12] of participants in the Safe Harbour scheme. Amongst other things, the listing identifies the enforcement and independent dispute resolution agency applicable to each participant.

33) Failure to comply with the Safe Harbour Privacy Principles and FAQs in the United States can result in an organisation being the subject of enforcement proceedings by the Federal Trade Commission. In the context of such proceedings, the Commission may impose significant financial penalties. It may also direct the strike-off of an organisation from the above-referred list, causing the organisation to lose its Safe Harbour status.

34) Recital 9 of the Commission Decision expressly recognises that it may need to be reviewed by the EU in the light of experience:

> *"The 'safe harbor' created by the Principles and the FAQs, may need to be reviewed in the light of experience, of developments concerning the protection of privacy in circumstances in which technology is constantly making easier the transfer and processing of personal data and in the light of reports on implementation by enforcement authorities involved."*

The DP Commissioner notes that a detailed review of the operation and effectiveness of the Safe Harbour scheme is presently underway and that changes to the scheme are the subject of ongoing negotiations between the Commission and the United States.

35) Article 4 of the Commission Decision provides:

> *"This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the*

[12] http://safeharbor.export.gov/list.aspx

Principles and the FAQs is overtaken by the requirements of US legislation."

36) Obviously the form of review and/or adaptations contemplated by Article 4 will occur at an EU and/or EU-US level. The DP Commissioner does not believe that it is his role to pre-empt what the outcome of the current review may be.

37) The Safe Harbour Principles set out at Annex 1 of the Commission Decision expressly state that:

> *"adherence to these principles may be limited (a) to the extent necessary to meet national security, public interest or law enforcement requirements ...."* .

38) The preamble to the Principles:

> *"US law will apply to questions of interpretation and compliance with the Safe Harbour Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbour organisations, except where organisations have committed to cooperate with European Data Protection Authorities ..."* .

39) Under Article 3 of the Commission Decision, a national Data Protection Authority can direct the suspension of data flows to an entity that has self-certified its adherence to the safe harbour principles in two specific scenarios:

(i) Where a relevant US enforcement authority has determined that the receiving entity is violating the safe harbour principles; or,

(ii) Where the following circumstances arise:

(a) There is a substantial likelihood that the Principles are being violated;

(b) There is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue;

(c) The continuing transfer would create an imminent risk of grave harm to data subjects; and,

(d) The competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

40) It is clear that (i) has no application to this case. So far as (ii) is concerned, the position is as follows.

41) In this case, no evidence was put before the DP Commissioner by the Applicant on which the DP Commissioner could have concluded that there was a *substantial* likelihood that the Safe Harbour Principles were in fact being violated specifically in the case of the data transfers referenced by the Applicant, i.e. data transfers between Facebook Ireland Limited and Facebook Inc. On the contrary, the Applicant's complaint was presented in generalised and essentially speculative terms. It is also of note that the Applicant did not adduce evidence to suggest that there was an imminent risk of grave harm to him, or that any of *his* data had been or was likely to be accessed by the National Security Agency. Rather, the complaint appeared to be made in a representative capacity on behalf of Facebook subscribers' generally.

42) Equally, the Applicant put forward no factual or other material on which the DP Commissioner could reasonably have concluded that the enforcement mechanisms provided for under the Safe Harbour Privacy Principles were not addressing (and would not address) the issues raised insofar as they affected the Applicant, or that the relevant enforcement and/or dispute resolution agency would not "take adequate and timely steps to settle the case at issue". Indeed, it is clear that, as at the date of submission of his complaint to the DP Commissioner, the Applicant had not sought to have recourse to the enforcement mechanisms provided for under the Safe Harbour Privacy Principles.[13]

[13] It appears that the Applicant may have sought to engage the Safe Harbour dispute resolution mechanism after the DP Commissioner had declined to investigate his complaint, and after the Applicant had already commenced judicial review proceedings against the DP Commissioner in the Irish High Court. At the hearing of the judicial

43) Nor is it clear how the DP Commissioner could himself have investigated or determined whether, for example, the NSA was accessing Facebook subscriber data at all, or in a way, or to an extent, that was not consistent with the Safe Harbour Privacy Principles and/or national or European data protection law. As noted at paragraphs 15, 23 and 25 of his First Affidavit, the DP Commissioner did in fact obtain confirmation from Facebook Ireland Limited (being the transferring party referenced by the Applicant) that the media reports on which the Applicant's complaint rested (being reports to the effect that the NSA was in a position to obtain direct and unhindered access to bulk data held on servers located in the United States relating to Facebook subscribers) were not correct.

44) Against this backdrop, and in circumstances where the EU Commission was already engaged in a substantial review of the operation of the Safe Harbour scheme with a view to effecting material changes to that scheme, the DP Commissioner took the view that the Applicant's complaint should properly be addressed at EU level and not by a national data protection commissioner.

The scope of the DP Commissioner's role in domestic law

45) It may be of assistance to the Court to make some observations on the legal nature of the DP Commissioner under Irish law. The DP Commissioner has jurisdiction to make decisions in respect of complaints that have first been admitted to investigation. Where a party to whom a decision is directed is dissatisfied, they may avail of a statutory appeal mechanism under which the decision will be the subject of a review by the Circuit Court. The DP Commissioner cannot award damages to a complainant. The fact that a complaint has been made to the DP Commissioner does not preclude a member of the public from litigating a grievance against someone who he believes has misused his data. By way of example Section 7 of the DP Acts provides that:

---

review proceedings on 30 April 2014, the Applicant produced, for the first time, a copy email dated 2 December 2013, received by him from TRUSTe, the dispute resolution entity named in Facebook Inc.'s Safe Harbour certificate. A request made by the Applicant to admit that email in evidence was denied by the Court on the basis that it post-dated the DP Commissioner's consideration of the Applicant's complaint. The Applicant's email, to which TRUSTe was replying, has not been available by the Applicant. (A copy of the email of 2 December 2013 is included as Attachment 6).

"For the purposes of the law of torts and to the extent that that law does not so provide, a person, being a data controller or a data processor, shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned..."

D) THE POSITION OF THE DP COMMISSIONER IN THIS CASE

46) The DP Commissioner formed the opinion that the Applicant's complaint should not be admitted to investigation on the basis that the complaint was not sustainable in law in light of:

(i) Section 11 of the DP Acts;

(ii) The Commission Decision;

(iii) the terms of the Safe Harbour Privacy Principles and FAQs; and,

(iv) Facebook's self-certified adherence to the Safe Harbour Principles and FAQs.

47) Put simply, the DP Commissioner considered that, in the particular circumstances that obtained, he was statutorily bound to accept that a transfer of subscriber data by Facebook Ireland Limited to Facebook Inc., undertaken under and in accordance with the Safe Harbour Privacy Principles and FAQs, is lawful, and remains lawful even where such data is accessed by national security authorities in the United States having regard to the express provision made in the Safe Harbour Privacy Principles and FAQs for third party access to the extent necessary to meet national security requirements.

48) Data protection is a rapidly developing area of the law and, in particular, there is an on-going and intensive debate taking place at an institutional level within the EU in relation to the capacity of the Safe Harbour Privacy Principles to provide adequate protection for the data privacy rights of citizens of the European Union whose personal data is transferred to the United States. The manner in which the EU interacts with the

United States in this context is clearly a matter that falls to be determined in the first instance by way of negotiations between the EU and the United States. Against that backdrop, and in the context of the development of specific legislative proposals for revisions to the existing Safe Harbour regime, a Communication[14] was issued by the European Commission on 27 November 2013, directed to the European Parliament and Council, in which the Commission recommended thirteen separate adjustments to the Safe Harbour Privacy Principles to address concerns raised about the operation of the Safe Harbour scheme in terms of transparency, availability of redress, enforcement, and access by United States authorities to transferred data. These recommendations remain the subject of discussion at EU level. They are also the subject of direct engagement between the EU and the United States in the context of ongoing dialogue between their respective justice and home affairs ministerial representatives.

49) So far as the subject matter of the Applicant's complaint is concerned, the Communication of 27 November 2013 contained recommendations under the heading "Access by US authorities", expressed in the following terms:

> *"12. Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.*
>
> *13. It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate."*

50) On the same date, a report[15] was published by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection. Amongst other things, the report presents certain

[14] http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

[15] http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

findings made by the EU co-chairs in connection with the legal basis on which surveillance programmes are in fact carried out by United States security agencies and the oversight and redress mechanisms to which they are subject.

51) For its part, the European Parliament has considered a report[16] dated 8 January 2014, prepared by the Parliament's Committee on Civil Liberties, Justice and Home Affairs on "the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." On the basis of its consideration of that report, the Parliament adopted a resolution[17] on 12 March 2014 in which (amongst other things) it called on the United States authorities to put forward a proposal for a new framework for transfers of personal data from the EU to the United States, to be substituted for the Safe Harbour framework, and which would meet EU law data protection requirements.

52) The DP Commissioner understands that, as of the date of delivery of these submissions, negotiations between the EU Commission and the United States in relation to changes demanded by the EU Commission to the Safe Harbour scheme remain ongoing.

53) From the outset of dealing with the Applicant's complaint the DP Commissioner emphasised the importance of the fact that the issues surrounding the 'PRISM' programme are the subject of active and ongoing engagement at an EU level and at inter-governmental level. Thus in the DP Commissioner's letter of reply dated 23 July 2013 he stated:

> *"We are aware of and welcome the fact that proportionality and oversight arrangements for programmes such as PRISM are to be the subject of high-level discussions between the EU and the USA."*[18]

[16] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0//EN

[17] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230

[18] See Attachment 7.

54) The DP Commissioner also noted the fact that the Applicant neither alleged, nor provided evidence, that any of his own personal data had been disclosed to US security authorities. Thus in the DP Commissioner's letter of reply dated 25 July 2013 he stated:

> *"In making this assessment, the DP Commissioner is mindful of the fact that there is no evidence – and you have not asserted – that your personal data has been disclosed to the US authorities."*[19]

55) By way of further illustration of the nature and extent of the on-going debate in this area, the documents that were adverted to in the affidavits and in the submissions of the Applicant before the Irish High Court include the following:

(i) Working Party Document on transfers of data to third countries[20] (24 July 1998);

(ii) Working Party Document on SWIFT[21] (22 November 2006);

(iii) Letter from Article 29 Data Protection Working Party to Vice President of the European Commission Viviane Reding[22] (13 August 2013);

(iv) Speech of European Data Protection Supervisor to EU Parliament[23] (7 October 2013);

(v) Communication from the European Commission to the Parliament and the Council[24] (27 November 2013);

(vi) Report on the Findings by the EU Co-Chairs of the ad hoc EU-US Working Group on Data Protection[25] (27 November 2013);

---

[19] See Attachment 8.

[20] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf

[21] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf

[22] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130813_letter_to_vp_reding_final_en.pdf

[23] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

[24] http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

(vii) Draft Report of European Parliament Committee on Civil Liberties, Justice and Home Affairs[26] (8 January 2014) (subsequently adopted as a resolution of the European Parliament on 12 March 2014);

(viii) Article 29 Data Protection Working Party Document on surveillance of electronic communications for intelligence and national security purposes[27] (10 April 2014);

(ix) Letter from Article 29 Data Working Party to Vice President of the European Commission Viviane Reading[28] (10 April 2014);

Even this list does not capture the full extent of the exchanges that have taken place (and the reports delivered) in relation to the operation of the Safe Harbour framework.

56) Given these ongoing and substantial developments at EU and inter-governmental level (to which the DP Commissioner is party in his capacity as a member of the Article 29 Working Group on Data Protection), we are a long way from the decision of the English courts in ***N.S. v Secretary of State for the Home Department***[29] where Member States were seeking to return asylum seekers to Greece even though they were fully aware that the Greek system had practically ground to a halt due to the fact that almost 90% of all illegal immigrants entering the EU in 2010 came into Greece (see para 87 of the decision). As set out above, in the present case, the DP Commissioner expressly noted the fact that proportionality and oversight arrangements for security programmes impacting on the data privacy rights of citizens are the subject of ongoing high-level discussions between the EU and the United States.

---

[25] http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

[26] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0//EN

[27] http://www.cnpd.public.lu/fr/publications/groupe-art29/wp215_en.pdf

[28] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

[29] [2013] QB 102; see Attachment 9.

57) Finally it may be noted that the recent decision of the CJEU in ***Digital Rights Ireland v Minister for Communications, Marine and Natural Resources***[30] was a case where the High Court in Ireland had been asked in plenary proceedings brought against the State to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005. The High Court in Ireland had made a reference to the ECJ to determine the validity of the Directive. Clearly it cannot be suggested that the DP Commissioner in this case had jurisdiction to declare any Irish or EU law to be invalid. The CJEU concluded that the Directive was invalid and stated:

> *"... the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data ..."* (para 54)

This is obviously a ruling that the Member States will have to pay regard to if they decide to amend the Commission Decision and to adjust the Safe Harbour Privacy Principles and FAQs previously agreed with the United States.

E) CONCLUSION

58) In conclusion, for all of the above reasons, it is submitted by the DP Commissioner that the answer to the first question posed by the Irish High Court is "Yes" and the answer to the second question (posed in the alternative) is "No".

Paul Anthony McDermott

[30] [2014] EUECJ C-293/12, (unreported, Grand Chamber, 8th April 2014); see Attachment 10.

APPENDIX

(Documents included as attachments to these submissions)

1. Letter from Maximillian Schrems to the Data Protection Commissioner, 25 June 2013

2. Data Protection Acts, 1988 & 2003 (consolidated version)

3. *Nowak v Data Protection Commissioner* [2013] 1 ILRM 207

4. *Maximillian Schrems v Data Protection Commissioner* [2014] IEHC 310

5. Jay, *Data Protection Law and Practice* (Sweet and Maxwell, 4th ed. 2012), Chapter 8

6. Email response from the Safe Harbour/TRUSTe Feedback and Resolution System, 2 December 2013

7. Letter from the Data Protection Commissioner to Maximillian Schrems, 23 July 2013

8. Letter from the Data Protection Commissioner to Maximillian Schrems, 25 July 2013

9. *N.S. v Secretary of State for the Home Department* [2013] QB 102

10. *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* [2014] EUECJ C-293/12, (unreported, Grand Chamber, 8th April 2014)

Signed: [redacted]

Damien Young
Philip Lee
Solicitors for the Data Protection Commissioner
7 – 8 Wilton Terrace
Dublin 2
IRELAND

24 October 2014

Date de réception : 23/01/2015

APPENDIX

(Documents included as attachments to these submissions)

1. Letter from Maximillian Schrems to the Data Protection Commissioner, 25 June 2013

2. Data Protection Acts, 1988 & 2003 (consolidated version)

3. *Nowak v Data Protection Commissioner* [2013] 1 ILRM 207

4. *Maximillian Schrems v Data Protection Commissioner* [2014] IEHC 310

5. Jay, *Data Protection Law and Practice* (Sweet and Maxwell, 4th ed. 2012), Chapter 8

6. Email response from the Safe Harbour/TRUSTe Feedback and Resolution System, 2 December 2013

7. Letter from the Data Protection Commissioner to Maximillian Schrems, 23 July 2013

8. Letter from the Data Protection Commissioner to Maximillian Schrems, 25 July 2013

9. *N.S. v Secretary of State for the Home Department* [2013] QB 102

10. *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* [2014] EUECJ C-293/12, (unreported, Grand Chamber, 8th April 2014)

1

To the
Data Protection Commissioner
Canal House, Station Road
Portarlington , Co. Laois
IRELAND

Maximilian Schrems
[redacted]

[redacted] June 25th 2013

Complaint against Facebook Ireland Ltd – 23 "PRISM"

To whom it may concern,

This is a formal complaint against "Facebook Ireland Ltd" under section 10 of the Irish DPA and at the same time also a request for a formal decision by the DPC. There is probable cause that "Facebook Ireland Ltd" is breaking the Irish DPA and the underlying Directive 94/46/EG and I kindly ask you to investigate the following complaint, inform me about your findings and make a legally binding decision after a conducting fair trial.

Facts of the Case:

I have been a user of "facebook.com" since 2008. Facebook stores large amounts of data about me (see previous – so far undecided – 22 complaints). My user ID is "hejdltiskeopzt", but my account is also visible under my name and registered to my email a0706826@unet.univie.ac.at. The Facebook service is provided to users outside of the USA and Canady by "Facebook Ireland Ltd" who is in my view partly a controller and partly a processor of my data (see other complaints filed in 2011). "Facebook Ireland Ltd" is not processing the data itself but transfers the data of its users to the USA where it is factually processed by "Facebook Inc".

"Facebook Inc" is subject to the "EU-USA Safe Harbor" system under which the users' data is transferred to the USA. There is no compulsory reason to transfer my personal data to the USA unless it is e.g. communicated to users in the USA. In general my data could also be held within the EU/EEA. "Facebook Ireland Ltd" seems to be using the services of "Facebook Inc" as a (sub-)processor voluntarily or only for economic reasons.

The British Guardian newspaper has now published documents by the US National Security Agency (NSA) that show that "Facebook Inc" is forwarding its user data to the NSA for reasons of espionage, national security and other matters. Facebook is listed in these documents as granting "mass access" to such data without any need for a probable cause since June 3rd 2009 under a program called "PRISM". The published documents indicate that "Facebook Inc" is participating (among other companies) in the PRISM program voluntarily. Other companies that provide similar services (like e.g. twitter) are not listed in the documents published by the Guardian. In addition, services were added over time, which is also pointing at a voluntary cooperation.

There are substantial reasons to assume that the facts revealed by the Guardian are correct. The involved companies have unanimously denied the direct access to its servers or even the knowledge of a program called PRISM. They only refer to numbers and laws that allow access to individual pieces of information in their statements. At the same time there was no such claim by the heads of the administration of the United States. If the reports were in essence false, one would have expected a quick and clear denial by the heads of the US government, but in fact the reactions have not at all been denying the allegations.

The first reactions by President Obama (http://on.wsj.com/14FU8eB) and the Director of National Intelligence James Clapper (http://tinyurl.com/litzz5g, http://tinyurl.com/mmos4fd and http://tinyurl.com/mwgu9d6) have not clearly denied direct access to the servers of "Facebook Inc" and the other companies involved. President Obama has explained details about access to communication data of "Verizon" but has not given any details on the accusations by the Guardian concerning the PRISM program. In different statements by James Clapper the NSA has further explained the rights to access under § 1881a U.S.C. While there are some clear words on the rights of US citizens, I was unable to find any clear statement that would deny access to or mass collection of data from non-US citizens. If the reports by the Guardian would be essentially wrong or if the published documents would not be genuine, it would have been logical to clearly and unambiguously reject the reports.

The companies involved are, according to their own statements, bound to secrecy under US laws ("gag orders"). This means that they are not allowed to say the truth about any such processing and are even bound to lie about such a program. Given this legal regime, the public statements by "Facebook Inc" are neither credible nor a reason to question the reports by the Guardian. So far neither "Facebook Inc" nor "Facebook Ireland Ltd" have issued a statement under an obligation to tell the truth or disclosed evidence that would prove the non-existence of the described cooperation with the NSA.

The statement that the NSA cannot "directly" access the servers of "Facebook Inc" reminds me very much of the facts in the "SWIFT" case. In this case the US government has installed a "black box" which was used to get full access to the financial transaction data stored by "SWIFT". The US government has thereby gained access to data in a way that is effectively equal to a direct access of servers.

- ***Summarizing the above: It is clear that "Facebook Ireland Ltd" is the controller or processor of my data. "Facebook Ireland Ltd" has outsourced the processing of my data to "Facebook Inc" and is therefore transferring my data to servers in the USA.***
- ***There is probable cause to believe that "Facebook Inc" is granting the NSA mass access to its servers that goes beyond merely individual requests based on probable cause.***
- ***The statements by "Facebook Inc" are in light of the US laws not credible, because "Facebook Inc" is bound by so-called "gag orders".***

- ***Therefore I ask the DPC to further clarify the facts and consult "Facebook Ireland Ltd" if they can prove by any means that the reports by the Guardian are false or substantially inaccurate.***
- ***As with all previous complaints against "Facebook Ireland Ltd", I understand that I will receive the outcome of such a clarification in line with my rights under Art 6 ECHR and the Irish law.***
- ***If there are any reasons to withhold such documents I hereby ask the DPC to limit such a restriction of my right to access to files to the minimum necessary and explain the reasons for a denial of access.***

2

24

Legal Arguments:

Controller:
To my understanding "Facebook Ireland Ltd" is the controller and/or processor of my data. This is also reflected by the terms of use on "facebook.com". "Facebook Inc" is correspondingly the processor or sub-processor that handles the data on behalf of "Facebook Ireland Ltd". Therefore "Facebook Ireland Ltd" is subject to the Irish Data Protection Act (DPA) and Directive 95/46/EC.

Purpose Limitation:
In Work Paper (WP) 128 on the Belgian financial services provider "SWIFT" the Article 29 Working Group has held that the mass use of *commercial* data for *investigative purposes* is a breach of the principle of purpose limitation. This argument equally applies to the data held by "Facebook Ireland Ltd" if such data is further used in masses for purposes like "terror prevention" or espionage. Therefore such usage by "Facebook Ireland Ltd" or its (sub-)processors is in breach of Article 6(1)(b) of Directive 95/46/EC and Section 2(1)(c)(ii) of the DPA.

As the Article 29 Working Group has already found in WP 128 the ECJ has interpreted Article 6 of the Directive 95/46/EC in light of Article 8 ECHR and has held that the forwarding and use for another purpose is interfering with the right to privacy under Article 8 ECHR and can therefore only be legitimate if it is "necessary in a democratic society" (see decisions C-465/00, C-138/01 and C-139/01 by the ECJ).

Proportionality:
In WP 128 the Article 29 Working party has said: *"The Working Party points out that even for the purposes of alleged terrorism investigations only specific and individualized data should be transferred by SWIFT on a case by case basis, in full compliance with data protection principles. As this is not the case, the current practice is not proportionate and thereby violates Article 6 (1) (c) of the Directive."*

Since the facts of the case are equivalent if now "Facebook Ireland Ltd" is (via "Facebook Inc") forwarding user data to the NSA in bulk it seems clear that the processing operations by "Facebook Ireland Ltd" are equally in breach of the DPA and Article 6(1) of Directive 95/46/EG.

Interpretation in line with WP 128: In the case of "SWIFT" the Article 29 Working Party has also considered the fact that the data was transferred to the US voluntarily: *"As a result by having decided to mirror all data processing activities in an operating center in the US, SWIFT placed itself in a foreseeable situation where it is subject to subpoenas under US law and where a processing of personal data has been organized in a way that appears to circumvent the structures and international agreements already in place."*

This argument must equally apply in the case of "Facebook Ireland Ltd". Because of its onward transfer of data to the US, "Facebook Ireland Ltd" has put itself in an equally foreseeable position in which the mass access of the NSA via its parent company "Facebook Inc" was even possible. Therefore "Facebook Ireland Ltd" cannot justify the situation with US regulations, if the arguments from the "SWIFT" decision are applied.

Transfer of Data to the US:
As mentioned above my data is processed in the US by "Facebook Inc". This means that thereby "Facebook Ireland Ltd" is transferring my data to a third country without an "adequate level of protection". Correspondingly Article 25 of Directive 95/26/EG and section 11 DPA apply to such transfers. A transfer to a third country without an adequate level or protection is only allowed under Article 25 of Directive 95/46/ if the fundamental rights and the right to data protection of the data subjects enjoy adequate factual and legal protecting in the third country.

The exceptions under section 11(4) DPA clearly do not apply. "Facebook Ireland Ltd" might argue that users have consented to such transfer, but users have surely not given an *informed* consented to the processing of their personal data in the US. "Facebook Ireland Ltd" has not informed its users about mass access and about

3

25

the cooperation with the NSA. To the contrary, "Facebook Inc" and "Facebook Ireland Ltd" is denying any such cooperation. Therefore there cannot be any informed consent.

As I know of no other basis that would make the transfer to the US legal under section 11 of the DPA or Directive 95/46/EG, I am further assuming that the transfer from "Apple Ireland" to "Apple Inc" is only done under the "Safe Harbor" system.

Safe Harbor:

"Facebook Inc" has joined the "Safe Harbor" (http://safeharbor.export.gov/companyinfo.aspx?id=18810) and has thereby self-certified that that it adheres to certain data protection principles (e.g. concerning the onward transfer of data). As far as I know the transfer of data to "Facebook Inc" is done solely on this legal basis.

Members of the "Safe Harbor" have pledged to limit onward transfer of data to third parties. In particular they have to adhere to the principles of "notice" and "choice". This means that there needs to be consent and proper information to data subjects if data is transferred. Both principles were not followed if user data was forwarded to the NSA in bulk. Concerning third party data stored on Facebook accounts, there is no practical possibility to adhere to such "choice" and "notice" principles.

Exception for "national security": Under the fourth paragraph of annex 1 of the "Safe Harbor" decision the adherence to the principles of the "Safe Harbor" can be limited for purposes of "national security".
I am therefore asking the DPC to inquire if "Facebook Inc" is forwarding my data to the NSA for compelling reasons of national security or if merely cooperating with the NSA voluntarily.
I further ask the DPC to inquire if this onward transfer of data to the NSA is in line with the exceptions from the "Safe Harbor" or if such an onward transfer is exceeding the exception and is therefore illegal. I kindly ask the DPC to consider the arguments below concerning the interpretation of this exception.

Exception for "statutory law": Under the fourth paragraph of annex 1 of the "Safe Harbor" decision the adherence to the principles of the "Safe Harbor" can be limited to comply with laws or even case law. According to the reports by the Guardian the mass access to the servers of "Facebook Inc" is bases on § 1881a U.S.C. (also known as 702 FISA).
I am therefore asking the DPC to inquire if Facebook's forwarding of my data to the NSA is necessary for compliance with § 1881a U.S.C. or if "Facebook Inc" is merely cooperating with the NSA voluntarily.
I further ask the DPC to inquire if this onward transfer of data to the NSA is in line with the exceptions from the "Safe Harbor" or if such an onward transfer is exceeding the exception and is therefore illegal. I kindly ask the DPC to consider the arguments below concerning the interpretation of this exception.

Interpretation of the "Safe Harbor" Decision:
The mere wording of the European Commission's Decision on the adequacy of the "Safe Harbor" from July 26th 2000 (L 2000/215, 7) could be interpreted in a way that the above mentioned exceptions would in reality be a "wildcard" that would allow the US to limit the application of the "Safe Harbor" decision by the European Commission as it pleases. Equally any form of data gathering for "national security" would be blankly exempt. In addition there is no definition or limitation of this "national security" exception. The exceptions under letter "a)" do also not include any limitation that would allow balancing these exceptions with the fundamental rights of data subjects.

If one would follow this interpretation, any form of onward mass transfer of personal data from an American processor to US authorities would be totally legal under EU law. Such mass surveillance would also be legal without any reasonable suspicion, without judicial overview and without any adherence to the fundamental rights equal to the ECHR and the CFR. Such an interpretation of the "Safe Harbor" could in no way be in line with Article 25 of Directive 95/46/EC, would be against recital 10 of the Directive 95/46/EC and would be in breach of Article 8 ECHR and Article 8 CFR.

But if the "Safe Harbor" decision is viewed within the hierarchy of the legal system, it seems clear that it is necessary to consider higher ranking fundamental rights and the directive when interpreting a decision of the European Commission. Otherwise one would imply that the European Commission's decision itself is not in line with these higher ranking laws.

Narrow interpretation in line with Directive 95/46/EC:
The "Safe Harbor" decision must be interpreted in line with Directive 95/46/EC, because the decision by the Commission cannot exceed the boundaries of the underlying law.

This means that when interpreting the exceptions above, it may only be interpreted in a way that the "adequacy" of the level of protection is in line with Article 25 of Directive 95/46/EG and in line with WP 12 of the Article 29 WP. Otherwise one would assume that the Commission has passed a decision that is in breach of Directive 95/46/EC. This possibility if covered below.

The adequacy of the protection of personal data does not only concern private use of data but also includes the public access and handling of such data, as the Article 29 WP has already pointed out in WP12 concerning contractual clauses: *"Article 6 of the Amsterdam Treaty also guarantees respect for the fundamental rights set out in the European Convention for the Protection of Human Rights and Fundamental Freedoms. In third countries similar limitations on the ability of the state to require the provision of personal data from companies (...) may not always be in place. (...) In some cases a contract is too frail an instrument to offer adequate data protection safeguards, and transfers to certain countries should not be authorised."*

In particular the DPC should investigate if a blanket exception for "national security" or "statutory law" of the US can be in line with Directive 95/46/EC and the users' fundamental rights under the European Union treaties. Until today it was primarily held that only the "national security" and laws of EU member states – and not any third country – can create exceptions for data processing. Otherwise the DPC would have to clarify in which case the "national security" or the law of a foreign country can be used to waive EU data protection laws.

If processing and a transfer of EU data for "national security" or the "laws" of third countries would be in line with Directive 95/46/EG this would also allow for a blanked transfer of data to any other foreign government (like Russia, China, Iran or North Korea) which can be in no way in line with EU legislation and the ECHR.

Narrow interpretation in line with Article 8 ECHR and Article 8 CFR:
The Irish DPA and Directive 95/46/EC have to be interpreted in line with the fundamental rights under the ECHR. This is not only derived from general legal principles but was also ruled by the ECJ (see e.g. § 21 of the ECJ's decision C-465/00, C-138/01 and C-139/01 of May 20th 2003). After the coming into force of the Lisbon treaty this must consequently also apply to the Charta of Fundamental Rights of the European Union (CFR).

An interference with the fundamental right to privacy can only be allowed under the ECHR if it is necessary in a democratic society and has to be additionally "proportionate" under the CFR. A mass transfer of European users' data to a foreign authority without any reasonable suspicion and with no effective legal remedy for the data subjects can in no way be in line with the fundamental rights we enjoy under the ECHR and the CFR. A mass access to content data without an individual justification and without individual judicial oversight cannot be in line with the fundamental rights we enjoy in the European Union. Consequently Directive 95/46/EC must be interpreted in a way that does not allow for such mass access.

In addition it would be highly questionable when the rights that are guaranteed under Article 8 ECHR and Article 8 CFR could be bypassed by forwarding EU data to third countries without such guarantees. Just like the principle of "non-refoulement" in asylum cases it has to be clear that a transfer of data to a third country that does not adhere to our understanding of fundamental rights would undermine our fundamental rights.

This issue becomes especially obvious if the results from the PRISM project are shared with European intelligence authorities as it was reported in many member states. In the end this would result in an "outsourcing" of government surveillance to territories outside of the scope of the ECHR and CFR. In contrast, my understanding is that the ECHR and the CFR require the EU and the member states to actively protect my fundamental rights – also against foreign countries.

→ ***I am therefor asking the DPC to ensure that the "Safe Harbor" Decision is interpreted in line with Directive 95/46/EG and fundamental rights. If it is necessary we recommend getting a preliminary ruling by the ECJ.***

Validity of the "Safe Harbor" Decision?

If the DPC is unable to interpret the "Safe Harbor" decision in line with Directive 95/46/EC, the ECHR and the CFR, the logical consequence would be that the decision by the European Commission is invalid. It is clear that the European Commission can only form a decision within the boundaries of such higher ranking laws.

The "Safe Harbor" decision was repeatedly and massively criticized, because there are reasons to believe that it does not guarantee an adequate level of data protection as described under Article 25 of Directive 95/46/EC. Until now the main point of criticism was the protection from companies in the US and what was frequently perceived as limited possibilities of enforcement. But Article 25 of the Directive 95/46/EC does not only cover the protection from private parties but covers a much broader scope of "adequacy" of the protection of fundamental rights (see references above). This also includes the protection from public authorities in a third country on a legal and factual level. This much broader scope must be observed when deciding about the "adequacy" of a transfer to a third country.

The initial adequacy decision by the European Commission on the "Safe harbor" from the year 2000 is especially problematic because of the massive changes in US legislation after the terror attacks of 9/11. Following these terrorist attacks the US have introduced many new laws and factual practices that hardly comply with European ideas of fundamental rights and the rule of law.

EU citizens are generally exempt from constitutional protection of their fundamental rights, since the US is still following the idea of "civil rights" (only applying to US citizens and people inside of the US) instead of "human rights". A "mass confiscation" of the EU citizens' data is therefore not covered by protections under the US constitution, but instead expressly allowed under § 1881a U.S.C. (also known as 702 FISA). There is no effective judicial oversight, because only the service provider – not the data subjects – can take legal action. The relevant FISA court forms its decisions behind closed doors and it has been reported that it has so far almost never refused any requested access to data. In addition, many other laws like the "Patriot Act" allow access to the data of European citizens in a way that is hardly in line with European fundamental rights. A more detailed elaboration on this matter is outside of the scope of this first submission on this matter.

While the adequacy decision by the European Commission might have been within the limits of Directive 95/46/EC when it was delivered in 2000, there are now serious doubts if the US is still giving "adequate" protection to the fundamental rights of European citizens on a legal and factual level. Therefore I have serious reason to believe that the adequacy decision by the European Commission might become subsequently invalid because of changes in the US legal system, as well as changes in the factual protection of EU nationals' privacy.

→ ***I am therefor asking the DPC to review the validity of the "Safe Harbor" decision and if necessary get a preliminary ruling by the ECJ on this matter, given the pan-European importance.***

Burden of Proof when transferring data to third countries:
Following the wording of Article 26(2) of Directive 95/46/EC and the systematic view on section 11 DPA the controller has the burden of proof for an adequate level of protection in a third country. This means that "Facebook Ireland Ltd" has to clarify and encounter my data is processed by "Facebook Inc" in a way that legally and factually ensures an adequate protection of my fundamental rights. This is also true within the "Safe Harbor" Framework (see e.g. decision by the German "Düsseldorfer Kreis" on April 28th/29th 2010).

If "Facebook Ireland Ltd" would refuse further clarification with reference to a "gag order" under US law, the only logical consequence would be that the transfer of personal data to "Facebook Inc" would need to be prohibited, because "Facebook Ireland Ltd" would not be able to demonstrate adequate safeguards in line with Article 26 of Directive 95/46/EG. This would clearly mean that a transfer to the US would be illegal.

- ***In summary it is clear that a "mass access" to personal data without a reasonable and specific suspicion against an individual is illegal under the ECHR and the CFR.***
- ***Such mass access would be in breach of the principle of "purpose limitation" as defined in Article 6(1)(b) of Directive 95/46/EC and Section 2(1)(c)(ii) of the DPA.***
- ***Such a wide access to personal data would further be illegal under the principle of proportionality under Article 6(1) of Directive 95/46/EG and the DPA.***
- ***In addition Directive 95/46/EC allows a transfer of personal data to a third country only if an "adequate level of protection" is guaranteed which is at least equal to the protection under the ECHR and the CFR.***
- ***A bulk transfer of personal data to the NSA would therefore be in breach of section 11 DPA and Articles 25 and 26 of Directive 95/46/EC as well as the ECHR and the CFR.***
- ***According to section 11 DPA and Article 26(2) of Directive 95/46/EC the controller has to ensure that adequate protections of the users' fundamental rights are in place. It is therefore upon "Facebook Ireland Ltd" to prove that the reported forwarding of data is not actually happening. If "Facebook Ireland Ltd" is unable to provide solid proof, any transfer to "Facebook Inc" in the US would need to be stopped.***

- ***I am therefor asking the DPC to investigate this complaint and if necessary stop the transfer of data to "Facebook Inc", if "Facebook Ireland Ltd" cannot prove that the reported forwarding of data to the NSA is not taking place.***

Thank you for protecting the fundamental rights of European citizens. I am available for further questions via [redacted] This complaint is digitally signed and therefore a legally binding complaint. Please note that similar complaints were and will be filed concerning other companies involved in the PRISM scandal in Ireland and other member states.

Kind Regards,

Maximilian Schrems

2

Number 25 *of* 1988

DATA PROTECTION ACT 1988

REVISED

Updated to 18 July 2014

This Revised Act is an administrative consolidation of the *Data Protection Act 1988.* It is prepared by the Law Reform Commission in accordance with its function under the *Law Reform Commission Act 1975* (3/1975) to keep the law under review and to undertake revision and consolidation of statute law.

All Acts up to and including *Health Service Executive (Financial Matters) Act 2014* (17/2014), enacted 17 July 2014, and all statutory instruments up to and including *Data Protection (Amendment) Act 2003 (Commencement) Order 2014* (S.I. No. 338 of 2014), made 18 July 2014, were considered in the preparation of this Revised Act.

Number 25 *of* 1988

DATA PROTECTION ACT 1988

REVISED

Updated to 18 July 2014

Introduction

This Revised Act presents the text of the Act as it has been amended since enactment, and preserves the format in which it was passed.

Related legislation

Data Protection Acts 1988 and 2003: This Act is one of a group of Acts included in this collective citation, to be construed together as one (*Data Protection (Amendment) Act 2003* (s. 23(2)). The Acts in the group are:

- *Data Protection Act 1988* (25/1988)
- *Data Protection Act 2003* (6/2003)

Annotations

This Revised Act is annotated and includes textual and non-textual amendments, statutory instruments made pursuant to the Act and previous affecting provisions.

An explanation of how to read annotations is available at www.lawreform.ie/annotations.

Material not updated in this revision

Where other legislation is amended by this Act, those amendments may have been superseded by other amendments in other legislation, or the amended legislation may have been repealed or revoked. This information is not represented in this revision but will be reflected in a revision of the amended legislation if one is available.

Where legislation or a fragment of legislation is referred to in annotations, changes to this legislation or fragment may not be reflected in this revision but will be reflected in a revision of the legislation referred to if one is available.

A list of legislative changes to any Act, and to statutory instruments from 2000, may be found in the Legislation Directory at www.irishstatutebook.ie.

Acts which affect or previously affected this revision

- *Health Identifiers Act 2014* (15/2014)

- *Criminal Justice (Forensic Evidence and DNA Database System) Act 2014* (11/2014)
- *Local Government Reform Act 2014* (1/2014)
- *Credit Reporting Act 2013* (45/2013)
- *Courts and Civil Law (Miscellaneous Provisions) Act 2013* (32/2013)
- *Health (Alteration of Criteria for Eligibility) Act 2013* (10/2013)
- *Personal Insolvency Act 2012* (44/2012)
- *Property Services (Regulation) Act 2011* (40/2011)
- *Student Support Act 2011* (4/2011)
- *National Asset Management Agency Act 2009* (34/2009)
- *Criminal Justice (Miscellaneous Provisions) Act 2009* (28/2009)
- *Nursing Homes Support Scheme Act 2009* (15/2009)
- *Criminal Justice (Mutual Assistance) Act 2008* (7/2008)
- *Medical Practitioners Act 2007* (25/2007)
- *Europol (Amendment) Act 2006* (37/2006)
- *Electoral (Amendment) Act 2006* (33/2006)
- *Planning and Development (Strategic Infrastructure) Act 2006* (27/2006)
- *Disability Act 2005* (14/2005)
- *Health Act 2004* (42/2004)
- *Public Service Management (Recruitment and Appointments) Act 2004* (33/2004)
- *Commissions of Investigation Act 2004* (23/2004)
- *Public Service Superannuation (Miscellaneous Provisions) Act 2004* (7/2004)
- *Civil Registration Act 2004* (3/2004)
- *Data Protection (Amendment) Act 2003* (6/2003)
- *Residential Institutions Redress Act 2002* (13/2002)
- *Customs and Excise (Mutual Assistance) Act 2001* (2/2001)
- *Planning and Development Act 2000* (30/2000)
- *Commission to Inquire into Child Abuse Act 2000* (7/2000)
- *British-Irish Agreement Act 1999* (1/1999)
- *Europol Act 1997* (38/1997)
- *Health (Provision of Information) Act 1997* (9/1997)
- *Refugee Act 1996* (17/1996)
- *Statistics Act 1993* (21/1993)

All Acts up to and including *Health Service Executive (Financial Matters) Act 2014* (17/2014), enacted 17 July 2014, were considered in the preparation of this revision.

Statutory instruments which affect or previously affected this revision

- *Data Protection Act 1988 (Commencement) Order 2014* (S.I. No. 337 of 2014)
- *European Union (Capital Requirements) Regulations 2014* (S.I. No. 158 of 2014)
- *European Union (Good Agricultural Practice for Protection of Waters) Regulations 2014* (S.I. No. 31 of 2014)
- *Data Protection Act 1988 (Section 2A) Regulations 2013* (S.I. No. 313 of 2013)
- *Data Protection Act 1988 (Section 2B) Regulations 2012* (S.I. No. 209 of 2012)
- *Data Protection Act 1988 (Section 2B) Regulations 2011* (S.I. No. 486 of 2011)
- *Finance (Transfer of Departmental Administration and Ministerial Functions) Order 2011* (S.I. No. 418 of 2011)
- *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011)
- *European Communities (Good Agricultural Practice for Protection of Waters) Regulations 2010* (S.I. No. 610 of 2010)
- *European Communities (Data Collection in the Fisheries Sector) Regulations 2010* (S.I. No. 132 of 2010)
- *Data Protection Act 1988 (Section 5(1)(d)) (Specification) Regulations 2009* (S.I. No. 421 of 2009)
- *European Communities (Payment Services) Regulations 2009* (S.I. No. 383 of 2009)
- *European Communities (Good Agricultural Practice For Protection of Waters) Regulations 2009* (S.I. No. 101 of 2009)
- *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008)
- *Data Protection (Processing of Genetic Data) Regulations 2007* (S.I. No. 687 of 2007)
- *Data Protection (Fees) Regulations 2007* (S.I. No. 658 of 2007)
- *Data Protection Act 1988 (Section 16(1)) Regulations 2007* (S.I. No. 657 of 2007)

- *European Communities (Good Agricultural Practice for Protection of Waters) Regulations 2005* (S.I. No. 788 of 2005)
- *European Communities (Good Agricultural Practice for Protection of Waters) Regulations 2006* (S.I. No. 378 of 2006)
- *Customs and Excise (Mutual Assistance) Act 2001 (Section 8) (Protection of Manual Data) Regulations 2004* (S.I. No. 254 of 2004)
- *European Communities (Clinical Trials on Medicinal Products For Human Use) Regulations 2004* (S.I. No. 190 of 2004)
- *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003)
- *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003)
- *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002)
- *European Communities (Data Protection) Regulations 2001* (S.I. No. 626 of 2001)
- *Data Protection (Registration) Regulations 2001* (S.I. No. 2 of 2001)
- *Data Protection (Fees) Regulations 1996* (S.I. No. 105 of 1996)
- *Data Protection Commissioner Superannuation Scheme 1993* (S.I. No. 141 of 1993)
- *Data Protection Act 1988 (Section 5(1)(d) (Specification) Regulations 1993* (S.I. No. 95 of 1993)
- *Data Protection (Fees) Regulations 1990* (S.I. No. 80 of 1990)
- *Data Protection Act 1988 (Section 5(1)(d)) (Specification) Regulations 1989* (S.I. No. 84 of 1989)
- *Data Protection (Access Modification) (Social Work) Regulations 1989* (S.I. No. 83 of 1989)
- *Data Protection (Access Modification) (Health) Regulations 1989* (S.I. No. 82 of 1989)
- *Data Protection Act 1988 (Restriction of Section 4) Regulations 1989* (S.I. No. 81 of 1989)
- *Data Protection (Registration) Regulations 1988* (S.I. No. 351 of 1988)
- *Data Protection (Registration Period) Regulations 1988* (S.I. No. 350 of 1988)
- *Data Protection Act (Commencement) Order 1988* (S.I. No. 349 of 1988)
- *Data Protection (Fees) Regulations 1988* (S.I. No. 347 of 1988)

All statutory instruments up to and including *Data Protection (Amendment) Act 2003 (Commencement) Order 2014* (S.I. No. 338 of 2014), made 18 July 2014, were considered in the preparation of this revision.

Number 25 *of* 1988

DATA PROTECTION ACT 1988

REVISED

Updated to 18 July 2014

ARRANGEMENT OF SECTIONS

Preliminary

34

35

ACTS REFERRED TO

Central Bank Act, 1971	1971, No. 24
Civil Service Commissioners Act, 1956	1956, No. 45
Civil Service Regulation Acts, 1956 and 1958	
Companies Act, 1963	1963, No. 33
Companies Acts, 1963 to 1987	
Defence Act, 1954	1954, No. 18
European Assembly Elections Act, 1977	1977, No. 30
European Assembly Elections Act, 1984	1984, No. 6
Interpretation Act, 1937	1937, No. 38
Local Government Act, 1941	1941, No. 23
Official Secrets Act, 1963	1963, No. 1
Petty Sessions (Ireland) Act, 1851	1851, c. 93
Prison Act, 1970	1970, No. 11
Public Offices Fees Act, 1879	1879, c. 58
Statutory Instruments Act, 1947	1947, No. 44

Number 25 *of* 1988

DATA PROTECTION ACT 1988

REVISED

Updated to 18 July 2014

AN ACT TO GIVE EFFECT TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981, AND FOR THAT PURPOSE TO REGULATE IN ACCORDANCE WITH ITS PROVISIONS THE COLLECTION, PROCESSING, KEEPING, USE AND DISCLOSURE OF CERTAIN INFORMATION RELATING TO INDIVIDUALS THAT IS PROCESSED AUTOMATICALLY. [13*th July*, 1988]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Annotations

Modifications (not altering text):

C1 Prospective affecting provision: application of collectively cited *Data Protection Acts 1988 and 2003* extended with any necessary modifications by *Criminal Justice (Miscellaneous Provisions) Act 2009* (28/2009), s. 23(2), not commenced as of date of revision.

Data Protection.

23.— (1) The Data Protection Commissioner is hereby designated as the national supervisory authority for the purposes of Article 60 of the Council Decision and Article 114 of the Schengen Convention.

(2) The Data Protection Acts 1988 and 2003 shall apply and have effect with any necessary modification to the collection, processing, keeping, use and disclosure of personal data for the purposes of the operation of the Council Decision and the Schengen Convention.

...

C2 Application of collectively cited *Data Protection Acts 1988 and 2003* restricted (28.01.2014) by *European Union (Good Agricultural Practice for Protection of Waters) Regulations 2014* (S.I. No. 31 of 2014), reg. 31.

Compliance with Data Protection Acts

31. The provision of information by a local authority, the Agency or the Minister for Agriculture, Food and the Marine in accordance with Article 27, 29 or 30 of these Regulations shall not be a breach of the Data Protection Acts, 1988 and 2003.

C3 Application of Act restricted by *Personal Insolvency Act 2012* (44/2012), s. 21A, as inserted (31.07.2013) by *Courts and Civil Law (Miscellaneous Provisions) Act 2013* (32/2013), s. 47, S.I. No. 286 of 2013.

Retention of information by Insolvency Service

37

21A. Notwithstanding the Data Protection Act 1988, the Insolvency Service shall retain such information or data obtained by it under this Act as is necessary for the performance of its functions under this Act.

C4 Application of collectively cited *Data Protection Acts 1988 and 2003* restricted (19.04.2013) by *Health (Alteration of Criteria for Eligibility) Act 2013* (10/2013), s. 8(4), S.I. No. 133 of 2013

Furnishing of personal data to and by Health Service Executive in certain circumstances.

8.— ...

(4) Notwithstanding anything contained in the Data Protection Acts 1988 and 2003, but subject to this section, a person who receives a request made in accordance with subsection (1), (2) or (3) shall comply with that request and shall do so in accordance with an agreement entered into under subsection (5) between the person and the person who made the request.

...

C5 Application of collectively cited *Data Protection Acts 1988 and 2003* restricted (27.06.2011) by *Student Support Act 2011* (4/2011), s. 28(1), S.I. No. 303 of 2011.

Processing of personal data.

28.— (1) Notwithstanding anything contained in the Data Protection Acts 1988 and 2003 or any other enactment, the data controller of a person listed in Schedule 2, or of a person prescribed for the time being under subsection (2) (in this subsection called "the first named person") shall on being requested to do so by the data controller of a person so listed or prescribed, process personal data kept by the first named person, or information extracted from such data, to the data controller of the other person so listed or prescribed for the time being, if the data controller of the first named person is satisfied that it will be used for a relevant purpose only.

...

C6 Application of collectively cited *Data Protection Acts 1988 and 2003* restricted (23.03.2010) by *European Communities (Data Collection in the Fisheries Sector) Regulations 2010* (S.I. No. 132 of 2010), reg. 7.

Obligations on certain public bodies

7. Notwithstanding the Data Protection Acts 1998 and 2003, the Sea Fisheries Protection Authority, the Marine Institute, Bord Iascaigh Mhara and the Minister shall make available to a data collection officer such data relating to activities referred to in Regulations 3, 4 or 5 as is available.

...

C7 Application of collectively cited *Data Protection Acts 1988 and 2003* restricted (21.12.2009) by *National Asset Management Agency Act 2009* (34/2009), s. 201, S.I. No. 545 of 2009.

Operation of Data Protection Acts 1988 and 2003.

201.— To avoid doubt, an obligation on a credit institution or any other person under this Act to disclose information to NAMA, a NAMA group entity or the NTMA extends to personal information, within the meaning of the Data Protection Acts 1988 and 2003.

...

C8 Application of collectively cited *Data Protection Acts 1988 and 2003* restricted (27.10.2009) by *Nursing Homes Support Scheme Act 2009* (15/2009), ss. 26 and 45, S.I. No. 423 of 2009.

Collection of monies advanced by way of ancillary State support.

26.— ...

(12) This section applies notwithstanding any provision of the Data Protection Acts 1988 and 2003.

...

Records.

38

45.— (1) Notwithstanding any provision of the Data Protection Acts 1988 to 2003, the Executive may, in accordance with this section, access and process any relevant records for the purposes of this Act.

...

C9 Application of Act restricted and application of Act confirmed (1.09.2008) by *Criminal Justice (Mutual Assistance) Act 2008* (7/2008), ss. 94, 107 and sch. 14, S.I. No. 338 of 2008.

Application in State of Ireland - US Treaty.

94.—(1) The Ireland - US Treaty has the force of law in its application in relation to the State.

...

(5) Article 7, in its application in relation to the use of personal data contained in evidence or information obtained under the Treaty by a person in the State, is without prejudice to the application of section 7 (duty of care owed by data controllers and data processors) of the Data Protection Act 1988 in respect of the use of such data.

(6) The Data Protection Acts 1988 and 2003 apply in relation to such data in respects other than those related to their use.

...

Personal data protection.

107.— (1) The provisions of the relevant international instrument have effect in respect of the use of personal data communicated to or otherwise obtained by a person in the State under the instrument.

2) Subsection (1) is without prejudice to the application of section 7 (duty of care owed by data controllers and data processors) of the Data Protection Act 1988 in respect of the use of such data.

3) The Data Protection Acts 1988 and 2003 apply in relation to such data in respects other than those relating to their use.

...

SCHEDULE 14

Text of Ireland/US Treaty of 18 January 2001, as applied by Instrument of 14 July 2005

...

Article 7

1. The Requesting Party may use any evidence or information obtained from the Requested Party:

(a) for the purpose of its criminal investigations and proceedings;

(b) for preventing an immediate and serious threat to its public security;

(c) in its non-criminal judicial or administrative proceedings directly related to investigations or proceedings:

(i) set forth in subparagraph (a); or

(ii) for which mutual legal assistance was rendered under Article 1 (1 bis)(a) of this Treaty;

(d) for any other purpose, if the evidence or information has been made public within the framework of proceedings for which they were transmitted, or in any of the situations described in subparagraphs (a), (b) and (c); and

(e) for any other purpose only with the prior consent of the Requested Party.

...

C10 Application of collectively cited *Data Protection Acts 1988 and 2003* restricted (1.11.2009) by *European Communities (Payment Services) Regulations 2009* (S.I. No. 383 of 2009), reg. 94.

Processing of personal data.

39

94. The processing, within the meaning of the Data Protection Acts 1988 and 2003, of personal data by a payment system or payment service provider is permitted for the purposes of the prevention, investigation and detection of payment fraud.

C11 Application of Act restricted (11.12.2006) by *Electoral (Amendment) Act 2006* (33/2006), s. 19, commenced on enactment.

List relating to draft register and register in force.

19.— Notwithstanding anything in the Data Protection Acts 1988 and 2003, a registration authority may, for the purposes of assisting in the preparation of a complete and accurate register of electors, prepare and publish, at any time after it publishes a draft register of electors in accordance with Rule 5 of the Second Schedule to the Act of 1992, a list, in such form and manner as the authority considers appropriate, of the names of all persons who are registered as electors in the register (in force at the time of publication of that draft register) but whose names are not included in that draft register.

C12 Application of collectively cited *Data Protection Acts 1988 and 2003* restricted (5.12.2005) by *Civil Registration Act 2004* (3/2004), s. 66, S.I. No. 764 of 2005, as amended

- by *Housing (Miscellaneous Provisions) Act 2009* (22/2009), s. 8 and sch. 2 part 8 item 1, not commenced as of date of revision;
- (1.01.2011) by *Civil Partnership and Certain Rights and Obligations of Cohabitants Act 2010* (24/2010), s. 21, S.I. No. 648 of 2010;
- (1.01.2009) by *Health Act 2008* (21/2008), s. 11, commenced as per s. 1(2);
- (17.12.2008) by *Social Welfare (Miscellaneous Provisions) Act 2008* (22/2008), s. 25, commenced on enactment;
- (1.01.2005) by *Health Act 2004* (42/2004), s. 75 and sch. 6 part 26 item 26, S.I. No. 887 of 2004.

Power of Ard-Chláraitheoir to give information to others.

66.—(1) Notwithstanding anything contained in the Data Protection Acts 1988 to 2003 or any other enactment, an tArd-Chláraitheoir may, after consultation with [...] the Minister for Social and Family Affairs, give such information as may be prescribed in relation to births, [marriages, civil partnerships, decrees of divorce, decrees of nullity of marriage, decrees of dissolution or decrees of nullity of civil partnership], registered under this Act or under any of the repealed enactments to—

(a) the Minister for Defence for the purpose of—

(i) the administration of schemes under the Defence Forces (Pensions) Acts 1932 to 1975, or

(ii) the administration of the Army Pensions Acts 1923 to 1980,

(b) the Minister for the Environment, Heritage and Local Government for the purpose of registration in a register under the Electoral Act 1992,

(c) the Minister for Foreign Affairs for the purpose of—

(i) determining entitlements to passports, or

(ii) verifying the identity of persons applying for or holding passports,

(d) the Minister for Justice, Equality and Law Reform for the purpose of determining the immigration or citizenship status of persons,

(e) the Minister for Social and Family Affairs for the purpose of—

(i) determining entitlement to, or control of, benefit under the Social Welfare (Consolidation) Act 1993, or

(ii) section 223 of that Act,

(f) the Minister for Transport for the purpose of the grant of driving licences and provisional licences under Part III of the Road Traffic Act 1961,

40

(g) the Minister for the purpose of the enforcement of regulations under section 31 of the Health Act 1947 and the Minister or [the Executive], hospital or other body or agency participating in any cancer screening programme (including any programme of breast or cervical cancer screening) authorised by the Minister, for the purpose of compiling and maintaining a record of the names, addresses and relevant dates of persons who, for public health reasons, may be invited to participate in any such programme,

(h) the Revenue Commissioners for the purpose of the administration of the Taxes Consolidation Act 1997, the Stamp Duties Consolidation Act 1999 and the Capital Acquisitions Tax Consolidation Act 2003,

(i) [the Executive] for the purpose of determining entitlement to a service provided for, by or under section 45[, 45A], 58, 59 or 61 of the Health Act 1970, and

(j) a housing authority (within the meaning of the Housing Act 1966) for the purpose of—

(i) the determination of entitlement to houses or grants under the Housing Acts 1966 to 2002,

(ii) the determination of a rent or other payment under section 58 of the Housing Act 1966, or

(iii) the preparation of a housing strategy under the Planning and Development Act 2000.

(2) In this section "information" means personal data (within the meaning of the Data Protection Acts 1988 and 2003) and information extracted from such data.

C13 Application of collectively cited *Data Protection Acts 1988 and 2003* restricted (1.05.2004) by *European Communities (Clinical Trials on Medicinal Products For Human Use) Regulations 2004* (S.I. No. 190 of 2004), reg. 48(3)(d).

Enforcement

48. — ...

(3) ...

(d) inspect and copy or extract information from any data (including personal data) within the meaning of the Data Protection Acts 1988 and 2003

...

C14 Application of Act extended with any necessary modifications (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

Unsolicited commercial communications.

9. ...

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

...

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

41

...

C15 Application of Act extended with any necessary modifications (22.02.2002) by *Customs and Excise (Mutual Assistance) Act 2001* (2/2001), ss. 5 and 9, S.I. No. 59 of 2002.

Application of Data Protection Act, 1988.

5.—(1) For the purposes of this Act, the CIS Convention and the Customs Co-operation Convention, the Data Protection Act, 1988, shall apply and have effect, with any necessary modifications, to the collection, processing, keeping, use or disclosure of personal data included in or received from the Customs Information System.

(2) Without prejudice to the generality of subsection (1), for the purposes of Article 21 of the CIS Convention, section 7 of the Data Protection Act, 1988, shall apply as regards the liability of the State for injury caused to a person through the use of the Customs Information System in the State.

(3) Without prejudice to the generality of subsection (1), for the purposes of Article 25 of the Customs Co-operation Convention, section 7 of the Data Protection Act, 1988, shall apply as regards the liability of the State for injury caused to a person through the processing of data communicated in the State.

...

Offences.

9.—Without prejudice to the generality of *section 5(1)*, any person who uses personal data from the Customs Information System other than for the purpose of the aim specified in Article 2(2) of the CIS Convention shall, save where such use is in accordance with and is subject to the conditions specified in Article 8(1) of that Convention, be guilty of an offence under the Data Protection Act, 1988.

C16 Application of Act restricted (20.11.2000) by *Refugee Act 1996* (17/1996), s. 11(5), S.I. No. 365 of 2000.

Investigation of application by Commissioner.

11.— ...

(5) Nothing in the Data Protection Act, 1988, shall be construed as prohibiting a person from giving to the Commissioner, on request by him or her, such information as is in the person's possession or control relating to the application.

C17 Act applied to certain bodies with any necessary modifications (2.12.1999) by *British-Irish Agreement Act 1999* (1/1999), s. 51, S.I. No. 377 of 1999.

Application of Data Protection Act, 1988.

51.— ...

(2) The Act of 1988 shall apply in relation to the Bodies with any necessary modifications and subject to the subsequent provisions of this section.

...

C18 Application of Act restricted (1.04.1997) by *Health (Provision of Information) Act 1997* (9/1997), s. 1(2), commenced on enactment. [Note that functions of specified bodies including health boards were transferred (1.01.2005) to the Health Service Executive by *Health Act 2004* (42/2004), s. 59, S.I. No. 887 of 2004].

Requests for and provision of information.

1.—...

(2) Nothing in the Data Protection Act, 1988, shall prevent the Minister for Health or a health board, hospital or other body or agency referred to in *subsection (1) (b)* from providing—

(*a*) to the Minister for Health, or to any other such health board, hospital or other body or agency, for the purposes of that programme, or

42

(*b*) for the purposes of inviting persons to participate in that programme,

any information provided under *subsection (1)*.

C19 Application of Act restricted (1.11.1994) by *Statistics Act 1993* (21/1993), s. 24(2), S.I. No. 323 of 1994.

Invitation to provide information on a voluntary basis.

24.—...

(2) Persons and undertakings may provide information and records, or copies thereof, which they may possess to the Director General or officers of statistics on invitation under the provisions of this Act notwithstanding anything contained in the Data Protection Act, 1988.

Editorial Notes:

E1 Previous affecting provision: application of collectively cited *Data Protection Acts 1988 and 2003* restricted (20.12.2010) by *European Communities (Good Agricultural Practice for Protection of Waters) Regulations 2010* (S.I. No. 610 of 2010), reg. 31; revoked (28.01.2014) by *European Union (Good Agricultural Practice for Protection of Waters) Regulations 2014* (S.I. No. 31 of 2014), reg. 3.

E2 Previous affecting provision: application of collectively cited *Data Protection Acts 1988 and 2003* restricted (31.03.2009) by *European Communities (Good Agricultural Practice For Protection of Waters) Regulations 2009* (S.I. No. 101 of 2009), reg. 31; revoked (20.12.2010) by *European Communities (Good Agricultural Practice for Protection of Waters) Regulations 2010* (S.I. No. 610 of 2010), reg. 2.

E3 Previous affecting provision: application of collectively cited *Data Protection Acts 1988 and 2003* restricted (1.08.2006) by *European Communities (Good Agricultural Practice for Protection of Waters) Regulations 2006* (S.I. No. 378 of 2006), reg. 31; revoked (31.03.2009) by *European Communities (Good Agricultural Practice For Protection of Waters) Regulations 2009* (S.I. No. 101 of 2009), reg. 2.

E4 Previous affecting provision: application of collectively cited *Data Protection Acts 1988 and 2003* restricted (1.02.2006) by *European Communities (Good Agricultural Practice for Protection of Waters) Regulations 2005* (S.I. No. 788 of 2005), reg. 31; revoked (1.08.2008) by *European Communities (Good Agricultural Practice for Protection of Waters) Regulations 2006* (S.I. No. 378 of 2006), reg. 2.

E5 Previous affecting provision: application of Act extended with any necessary modifications (1.10.1998) by *Europol Act 1997* (38/1997), s. 6, S.I. No. 345 of 1998, as amended (23.12.2006) by substitution of subs. (1) by *Europol (Amendment) Act 2006* (37/2006), s. 3, commenced on enactment; repealed (1.02.2013) by *Europol Act 2012* (53/2012), s. 17, S.I. No. 15 of 2013.

Preliminary

Interpretation and application of Act.

1.—(1) In this Act, unless the context otherwise requires—

F1['the Act of 2003' means the Data Protection (Amendment) Act 2003]

"appropriate authority" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

F1['automated data' means information that—

(*a*) is being processed by means of equipment operating automatically in response to instructions given for that purpose, or

(*b*) is recorded with the intention that it should be processed by means of such equipment;]

43

"back-up data" means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

F1[‘blocking’, in relation to data, means so marking the data that it is not possible to process it for purposes in relation to which it is marked;]

"civil servant" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

"the Commissioner" has the meaning assigned to it by *section 9* of this Act;

"company" has the meaning assigned to it by the Companies Act, 1963

"the Convention" means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January, 1981, the text of which is set out in the *First Schedule* to this Act;

"the Court" means the Circuit Court

F2[‘data’ means automated data and manual data;]

"data controller" means a person who, either alone or with others, controls the contents and use of personal data;

"data equipment" means equipment for processing data;

"data material" means any document or other material used in connection with, or produced by, data equipment;

"data processor" means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment;

"data subject" means an individual who is the subject of personal data;

F1[‘the Directive’ means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[(1)];]

F2[‘direct marketing’ includes direct mailing other than direct mailing carried out in the course of political activities by a political party or its members, or a body established by or under statute or a candidate for election to, or a holder of, elective political office;]

"disclosure", in relation to personal data, includes the disclosure of information extracted from such data and the transfer of such data but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his duties; and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall not be regarded as disclosed unless the other information is also disclosed;

F1[‘the EEA Agreement’means the Agreement on the European Economic Area signed at Oporto on 2 May 1992 as adjusted by the Protocol signed at Brussels on 17 March 1993;]

F1[‘enactment’ means a statute or a statutory instrument (within the meaning of the Interpretation Act 1937);]

"enforcement notice" means a notice under *section 10* of this Act;

F1[‘the European Economic Area’ has the meaning assigned to it by the EEA Agreement;]

[(1)] O.J. No. L 281/38 of 23.11.95, p.31.

44

"financial institution" means—

(*a*) a person who holds or has held a licence under section 9 of the Central Bank Act, 1971, or

(*b*) a person referred to in section 7 (4) of that Act;

"information notice" means a notice under *section 12* of this Act;

F3["local authority" means a local authority for the purposes of the Local Government Act 2001 (as amended by the Local Government Reform Act 2014);]

F1['manual data'means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;]
"the Minister" means the Minister for Justice;

F2['personal data' means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller;]

"prescribed", in the case of fees, means prescribed by regulations made by the Minister with the consent of the Minister for Finance and, in any other case, means prescribed by regulations made by the Commissioner with the consent of the Minister;

F2['processing' of or in relation to information or data, means performing any operation or set of operations on the information or data, whether or not by automatic means, including—

(*a*) obtaining, recording or keeping the information or data,

(*b*) collecting, organising, storing, altering or adapting the information or data,

(*c*) retrieving, consulting or using the information or data,

(*d*) disclosing the information or data by transmitting, disseminating or otherwise making it available, or

(*e*) aligning, combining, blocking, erasing or destroying the information or data;]

"prohibition notice" means a notice under *section 11* of this Act;

"the register" means the register established and maintained under *section 16* of this Act;

F4['relevant filing system' means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;]

F1['sensitive personal data' means personal data as to—

(*a*) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,

(*b*) whether the data subject is a member of a trade union,

(*c*) the physical or mental health or condition or sexual life of the data subject,

(*d*) the commission or alleged commission of any offence by the data subject, or

(*e*) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings;]

45

and any cognate words shall be construed accordingly.

(2) For the purposes of this Act, data are inaccurate if they are incorrect or misleading as to any matter of fact.

(3) (*a*) An appropriate authority, being a data controller or a data processor, may, as respects all or part of the personal data kept by the authority, designate a civil servant in relation to whom it is the appropriate authority to be a data controller or a data processor and, while the designation is in force—

(i) the civil servant so designated shall be deemed, for the purposes of this Act, to be a data controller or, as the case may be, a data processor, and

(ii) this Act shall not apply to the authority,

as respects the data concerned.

(*b*) Without prejudice to *paragraph (a)* of this subsection, the Minister for Defence may, as respects all or part of the personal data kept by him in relation to the Defence Forces, designate an officer of the Permanent Defence Force who holds a commissioned rank therein to be a data controller or a data processor and, while the designation is in force—

(i) the officer so designated shall be deemed, for the purposes of this Act, to be a data controller or, as the case may be, a data processor, and

(ii) this Act shall not apply to the Minister for Defence,

as respects the data concerned.

(*c*) For the purposes of this Act, as respects any personal data—

(i) where a designation by the relevant appropriate authority under *paragraph (a)* of this subsection is not in force, a civil servant in relation to whom that authority is the appropriate authority shall be deemed to be its employee and, where such a designation is in force, such a civil servant (other than the civil servant the subject of the designation) shall be deemed to be an employee of the last mentioned civil servant,

(ii) where a designation under *paragraph (b)* of this subsection is not in force, a member of the Defence Forces shall be deemed to be an employee of the Minister for Defence and, where such a designation is in force, such a member (other than the officer the subject of the designation) shall be deemed to be an employee of that officer, and

(iii) a member of the Garda Síochána (other than the Commissioner of the Garda Síochána) shall be deemed to be an employee of the said Commissioner.

F1[(3A) A word or expression that is used in this Act and also in the Directive has, unless the context otherwise requires, the same meaning in this Act as it has in the Directive.

(3B) (*a*) Subject to any regulations under section 15(2) of this Act, this Act applies to data controllers in respect of the processing of personal data only if—

(i) the data controller is established in the State and the data are processed in the context of that establishment, or

(ii) the data controller is established neither in the State nor in any other state that is a contracting party to the EEA Agreement but makes use of equipment in the State for processing the data otherwise than for the purpose of transit through the territory of the State.

46

(*b*) For the purposes of paragraph (*a*) of this subsection, each of the following shall be treated as established in the State:

(i) an individual who is normally resident in the State,

(ii) a body incorporated under the law of the State,

(iii) a partnership or other unincorporated association formed under the law of the State, and

(iv) a person who does not fall within subparagraphs (i), (ii) or (iii) of this paragraph, but maintains in the State—

(I) an office, branch or agency through which he or she carries on any activity, or

(II) a regular practice,

and the reference to establishment in any other state that is a contracting party to the EEA Agreement shall be construed accordingly.

(*c*) A data controller to whom paragraph (*a*)(ii) of this subsection applies must, without prejudice to any legal proceedings that could be commenced against the data controller, designate a representative established in the State.

(3C) Section 2 and sections 2A and 2B (which sections were inserted by the Act of 2003) of this Act shall not apply to—

(*a*) data kept solely for the purpose of historical research, or

(*b*) other data consisting of archives or departmental records (within the meaning in each case of the National Archives Act 1986),

and the keeping of which complies with such requirements (if any) as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects.]

(4) This Act does not apply to—

(*a*) personal data that in the opinion of the Minister or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State,

(*b*) personal data consisting of information that the person keeping the data is required by law to make available to the public, or

(*c*) personal data kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes.

F1[(5) (*a*) A right conferred by this Act shall not prejudice the exercise of a right conferred by the Freedom of Information Act 1997.

(*b*) The Commissioner and the Information Commissioner shall, in the performance of their functions, co-operate with and provide assistance to each other.]

Annotations

Amendments:

F1 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 2, S.I. No. 207 of 2003.

47

F2 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 2, S.I. No. 207 of 2003.

F3 Substituted (1.06.2014) by *Local Government Act 2014* (1/2014), s. 5(8) and sch. 2 part 6, S.I. No. 214 of 2014.

F4 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 2, S.I. No. 207 of 2003.

Modifications (not altering text):

C20 Prospective affecting provision: section applied with modifications by *Criminal Justice (Forensic Evidence and DNA Database System) Act 2014* (11/2014), s. 123(1), (2)(a), not commenced as of date of revision.

Application of Act of 1988

123. (1) The Act of 1988 shall, with the modifications specified in subsection (2) and any other necessary modifications, apply to the processing of personal data supplied or received pursuant to—

(a) Chapter 2,

(b) Chapter 3, or

(c) an Article 7 request,

and, for the purposes of the foregoing application of the Act of 1988, references in it to that Act or the provisions of that Act shall, unless the context otherwise requires, be construed as including references to—

(i) Chapter 2 or the provisions of that Chapter,

(ii) Chapter 3 or the provisions of that Chapter, and

(iii) Chapter 3 of Part 5 of the Act of 2008 insofar as that Chapter applies to an Article 7 request or the provisions of that Chapter insofar as they apply to such a request.

(2) The modifications of the Act of 1988 referred to in subsection (1) are the following, namely—

(a) in section 1(1), the insertion of the following definitions:

'Act of 2008' means the Criminal Justice (Mutual Assistance) Act 2008;

'Act of 2014' means the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014;

'Agreement with Iceland and Norway', 'Council Decision', 'dactyloscopic data', 'designated state', 'European Union or international instrument', 'Member State' and 'relevant European Union or international instrument' have the meanings they have in section 109 of the Act of 2014;

'Article 7 request' means a request made or received under Chapter 3 of Part 5 of the Act of 2008 pursuant to Article 7 of the Council Decision or that Article insofar as it is applied by Article 1 of the Agreement with Iceland and Norway;

'Central Authority' has the meaning it has in section 2(1) of the Act of 2008;

'data protection authority', in relation to a designated state, means the authority in that designated state that is designated by that designated state to be the independent data protection authority of that designated state for the purposes of a European Union or international instrument;

'DNA' means deoxyribonucleic acid;

'national contact point', in relation to a relevant European Union or international instrument, has the meaning it has in section 109 of the Act of 2014;

'processing' has the meaning it has in this Act and shall include the sending or receipt, as the case may be, of a notification under section 113 (2), 114 (3), 115 (2), 116 (3), 119 (2) or 120 (2) of the Act of 2014.

...

48

C21 The definition of "financial institution", defined above, is extended (31.03.2014) by *European Union (Capital Requirements) Regulations 2014* (S.I. No. 158 of 2014), reg. 152.

Continuation of contravention of Regulations

152. Notwithstanding Regulation 7(1), the references, however expressed, to the holder of a licence under section 9 of the Act of 1971, in—

(a) sections 19 to 26, section 28, sections 31 to 42 or section 58 of the Act of 1971,

(b) section 27, sections 49 to 51, sections 90, 108, 117, 134 or 140 of the Central Bank Act 1989 (No. 16 of 1989), or

(c) any other enactment which was in force on 1 January 1993,

shall be construed so as to include any person who, but for the application of Regulation 7(1), was or would have been required to hold a licence under section 9 of the Act of 1971.

C22 Functions transferred and references to "Department of Finance" and "Minister for Finance" construed (29.07.2011) by *Finance (Transfer of Departmental Administration and Ministerial Functions) Order 2011* (S.I. No. 418 of 2011), arts. 2, 3, 5 and sch. 1 part 2, in effect as per art. 1(2), subject to transitional provisions in arts. 6-9.

2. (1) The administration and business in connection with the performance of any functions transferred by this Order are transferred to the Department of Public Expenditure and Reform.

(2) References to the Department of Finance contained in any Act or instrument made thereunder and relating to the administration and business transferred by paragraph (1) shall, on and after the commencement of this Order, be construed as references to the Department of Public Expenditure and Reform.

3. The functions conferred on the Minister for Finance by or under the provisions of —

(a) the enactments specified in Schedule 1, and

(b) the statutory instruments specified in Schedule 2,

are transferred to the Minister for Public Expenditure and Reform.

...

5. References to the Minister for Finance contained in any Act or instrument under an Act and relating to any functions transferred by this Order shall, from the commencement of this Order, be construed as references to the Minister for Public Expenditure and Reform.

...

Schedule 1

Enactments

...

Part 2

1922 to 2011 Enactments

Number and Year	Short Title	Provision
(1)	(2)	(3)
...	...	...
No. 25 of 1988	Data Protection Act 1988	Sections 1 and 33(1); Second Schedule, paragraph 9
...	...	...

C23 Application of section extended (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

Unsolicited commercial communications.

9. ...

49

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

(8) Section 1(1) of the Act applies as if the following definition were inserted: " 'Regulations of 2003' means the European Communities (Directive 2000/31/EC) Regulations 2003;"

...

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

...

Editorial Notes:

E6 Prospective affecting provision: as provided by *Health Identifiers Act 2014* (15/2014), s. 27(1), (2), not commenced as of date of revision, a living individual's individual health identifier held by certain persons is considered personal data for the purposes of the *Data Protection Acts 1988 and 2003*. This shall not be construed to prevent a living individual's individual health identifier held by a person other than the certain persons from being personal data in accordance with the provisions of those Acts.

E7 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35, subject to transitional provisions in reg. 34.

E8 Previous affecting provision: definitions for "Directive", "EEA Agreement", "Enactment" and "European Economic Area" inserted (1.04.2002) by *European Communities (Data Protection) Regulations 2001* (S.I. No. 626 of 2001), reg. 2(a); substituted as per F-note above.

E9 Previous affecting provision: subs. (5) inserted (1.04.2002) by *European Communities (Data Protection) Regulations 2001* (S.I. No. 626 of 2001), reg. 2(b); substituted as per F-note above.

Protection of Privacy of Individuals with regard to Personal Data

Collection, processing, keeping, use and disclosure of personal data.

2.—F5[(1) A data controller shall, as respects personal data kept by him or her, comply with the following provisions:

(*a*) the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly,

(*b*) the data shall be accurate and complete and, where necessary, kept up to date,

50

(*c*) the data—

(i) shall have been obtained only for one or more specified, explicit and legitimate purposes,

(ii) shall not be further processed in a manner incompatible with that purpose or those purposes,

(iii) shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed, and

(iv) shall not be kept for longer than is necessary for that purpose or those purposes,

(*d*) appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.]

(2) A data processor shall, as respects personal data processed by him, comply with *paragraph (d)* of *subsection (1)* of this section.

(3) *Paragraph (a)* of the said *subsection (1)* does not apply to information intended for inclusion in data, or to data, kept for a purpose mentioned in *section 5 (1) (a)* of this Act, in any case in which the application of that paragraph to the data would be likely to prejudice any of the matters mentioned in the said *section 5 (1) (a)*.

(4) *Paragraph (b)* of the said *subsection (1)* does not apply to backup data.

(5) F6[(*a*) Subparagraphs (ii) and (iv) of paragraph (*c*) of the said subsection (1) do not apply to personal data kept for statistical or research or other scientific purposes, and the keeping of which complies with such requirements (if any) as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects, and,]

(*b*) the data or, as the case may be, the information constituting such data shall not be regarded for the purposes of *paragraph (a)* of the said subsection as having been obtained unfairly by reason only that its use for any such purpose was not disclosed when it was obtained,

if the data are not used in such a way that damage or distress is, or is likely to be, caused to any data subject.

(6) F7[...]

F8[(7) Where—

(*a*) personal data are kept for the purpose of direct marketing, and

(*b*) the data subject concerned requests the data controller in writing—

(i) not to process the data for that purpose, or

(ii) to cease processing the data for that purpose,

then—

(I) if the request is under paragraph (*b*)(i) of this subsection, the data controller—

(A) shall, where the data are kept only for the purpose aforesaid, as soon as may be and in any event not more than 40 days after the request has been given or sent to him or her, erase the data, and

57

(B) shall not, where the data are kept for that purpose and other purposes, process the data for that purpose after the expiration of the period aforesaid,

(II) if the request is under paragraph (*b*)(ii) of this subsection, as soon as may be and in any event not more than 40 days after the request has been given or sent to the data controller, he or she—

(A) shall, where the data are kept only for the purpose aforesaid, erase the data, and

(B) shall, where the data are kept for that purpose and other purposes, cease processing the data for that purpose,

and

(III) the data controller shall notify the data subject in writing accordingly and, where appropriate, inform him or her of those other purposes.

(8) Where a data controller anticipates that personal data, including personal data that is required by law to be made available to the public, kept by him or her will be processed for the purposes of direct marketing, the data controller shall inform the persons to whom the data relates that they may object, by means of a request in writing to the data controller and free of charge, to such processing.]

Annotations

Amendments:

F5 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 3(a), S.I. No. 207 of 2003. Amendments to section pursuant to 6/2003, s. 23 in respect of manual data held in relevant filing systems on the passing of 6/2003 commenced (24.10.2007) by s. 23(4), subject to transitional provision in subs. (5).

F6 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 3(b), S.I. No. 207 of 2003. Amendments to section pursuant to 6/2003, s. 23 in respect of manual data held in relevant filing systems on the passing of 6/2003 commenced (24.10.2007) by s. 23(4), subject to transitional provision in subs. (5).

F7 Deleted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 3(c), S.I. No. 207 of 2003. Amendments to section pursuant to 6/2003, s. 23 in respect of manual data held in relevant filing systems on the passing of 6/2003 commenced (24.10.2007) by s. 23(4), subject to transitional provision in subs. (5).

F8 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 3(d), S.I. No. 207 of 2003. Amendments to section pursuant to 6/2003, s. 23 in respect of manual data held in relevant filing systems on the passing of 6/2003 commenced (24.10.2007) by s. 23(4), subject to transitional provision in subs. (5).

Modifications (not altering text):

C24 Prospective affecting provision: section applied with modifications by *Criminal Justice (Forensic Evidence and DNA Database System) Act 2014* (11/2014), s. 123(1), (2)(b), not commenced as of date of revision.

Application of Act of 1988

123. (1) The Act of 1988 shall, with the modifications specified in subsection (2) and any other necessary modifications, apply to the processing of personal data supplied or received pursuant to—

(a) Chapter 2,

(b) Chapter 3, or

52

(c) an Article 7 request,

and, for the purposes of the foregoing application of the Act of 1988, references in it to that Act or the provisions of that Act shall, unless the context otherwise requires, be construed as including references to—

(i) Chapter 2 or the provisions of that Chapter,

(ii) Chapter 3 or the provisions of that Chapter, and

(iii) Chapter 3 of Part 5 of the Act of 2008 insofar as that Chapter applies to an Article 7 request or the provisions of that Chapter insofar as they apply to such a request.

(2) The modifications of the Act of 1988 referred to in subsection (1) are the following, namely—

...

(b) in section 2, the insertion of the following subsections after subsection (1):

"(1A) A data controller (including a national contact point) shall in order to comply with subsection (1) (b) as respects personal data kept by him or her also comply with section 125 of the Act of 2014 in respect of those data.

(1B) For the purposes of subparagraphs (i) and (ii) of subsection (1) (c), the processing of personal data supplied or received pursuant to—

(a) Chapter 2 of Part 12 of the Act of 2014, or

(b) Chapter 3 of that Part of that Act,

is deemed to be a purpose compatible with the purpose for which those data were obtained.",

...

C25 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

Editorial Notes:

E10 Prospective affecting provision: subs. (1)(d) applied to a deceased individual's relevant information as it does to a living individual's relevant information by *Health Identifiers Act 2014* (15/2014), s. 27(3), not commenced as of date of revision.

F9[Processing of personal data.

2A.—(1) Personal data shall not be processed by a data controller unless section 2 of this Act (as amended by the Act of 2003) is complied with by the data controller and at least one of the following conditions is met:

(*a*) the data subject has given his or her consent to the processing or, if the data subject, by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian or a grandparent, uncle, aunt, brother or sister of the data subject and the giving of such consent is not prohibited by law,

53

(*b*) the processing is necessary—

(i) for the performance of a contract to which the data subject is a party,

(ii) in order to take steps at the request of the data subject prior to entering into a contract,

(iii) for compliance with a legal obligation to which the data controller is subject other than an obligation imposed by contract, or

(iv) to prevent—

(I) injury or other damage to the health of the data subject, or

(II) serious loss of or damage to property of the data subject,

or otherwise to protect his or her vital interests where the seeking of the consent of the data subject or another person referred to in paragraph (*a*) of this subsection is likely to result in those interests being damaged,

(*c*) the processing is necessary—

(i) for the administration of justice,

(ii) for the performance of a function conferred on a person by or under an enactment,

(iii) for the performance of a function of the Government or a Minister of the Government, or

(iv) for the performance of any other function of a public nature performed in the public interest by a person,

(*d*) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

(2) The Minister may, after consultation with the Commissioner, by regulations specify particular circumstances in which subsection (1)(*d*) of this section is, or is not, to be taken as satisfied.]

Annotations

Amendments:

F9 Inserted (1.07.2003) by *Data Protection Amendment Act 2003* (6/2003), s. 4, S.I. No. 207 of 2003. Commenced (24.10.2007) in respect of manual data held in relevant filing systems on the passing of 6/2003 by s. 23(4), subject to transitional provision in subs. (5).

Editorial Notes:

E11 Power pursuant to subs. (1)(d) and (2) exercised (22.06.2013) by *Data Protection Act 1988 (Section 2A) Regulations 2013* (S.I. No. 313 of 2013).

E12 Previous affecting provision: section inserted (1.04.2002) by *European Communities (Data Protection) Regulations 2001* (S.I. No. 626 of 2001), reg. 3; substituted as per F-note above.

F10[Processing of sensitive personal data.

2B.—(1) Sensitive personal data shall not be processed by a data controller unless:

(*a*) sections 2 and 2A (as amended and inserted, respectively, by the Act of 2003) are complied with, and

SY

(*b*) in addition, at least one of the following conditions is met:

(i) the consent referred to in paragraph (*a*) of subsection (1) of section 2A (as inserted by the *Act of 2003*) of this Act is explicitly given,

(ii) the processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment,

(iii) the processing is necessary to prevent injury or other damage to the health of the data subject or another person or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where—

(I) consent to the processing cannot be given by or on behalf of the data subject in accordance with section 2A(1)(*a*) (inserted by the Act of 2003) of this Act, or

(II) the data controller cannot reasonably be expected to obtain such consent,

or the processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of, or damage to, the property of another person, in a case where such consent has been unreasonably withheld,

(iv) the processing—

(I) is carried out in the course of its legitimate activities by any body corporate, or any unincorporated body of persons, that—

(A) is not established, and whose activities are not carried on, for profit, and

(B) exists for political, philosophical, religious or trade union purposes,

(II) is carried out with appropriate safeguards for the fundamental rights and freedoms of data subjects,

(III) relates only to individuals who either are members of the body or have regular contact with it in connection with its purposes, and

(IV) does not involve disclosure of the data to a third party without the consent of the data subject,

(v) the information contained in the data has been made public as a result of steps deliberately taken by the data subject,

(vi) the processing is necessary—

(I) for the administration of justice,

(II) for the performance of a function conferred on a person by or under an enactment, or

(III) for the performance of a function of the Government or a Minister of the Government,

(vii) the processing—

(I) is required for the purpose of obtaining legal advice or for the purposes of, or in connection with, legal proceedings or prospective legal proceedings, or

(II) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

(viii) the processing is necessary for medical purposes and is undertaken by—

(I) a health professional, or

(II) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health professional,

(ix) the processing is necessary in order to obtain information for use, subject to and in accordance with the Statistics Act 1993, only for statistical, compilation and analysis purposes,

(x) the processing is carried out by political parties, or candidates for election to, or holders of, elective political office, in the course of electoral activities for the purpose of compiling data on people's political opinions and complies with such requirements (if any) as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects,

(xi) the processing is authorised by regulations that are made by the Minister and are made for reasons of substantial public interest,

(xii) the processing is necessary-for the purpose of the assessment, collection or payment of any tax, duty, levy or other moneys owed or payable to the State and the data has been provided by the data subject solely for that purpose,

(xiii) the processing is necessary for the purposes of determining entitlement to or control of, or any other purpose connected with the administration of any benefit, pension, assistance, allowance, supplement or payment under the Social Welfare (Consolidation) Act 1993, or any nonstatutory scheme administered by the Minister for Social, Community and Family Affairs.

(2) The Minister may by regulations made after consultation with the Commissioner—

(*a*) exclude the application of subsection (1)(*b*)(ii) of this section in such cases as may be specified, or

(*b*) provide that, in such cases as may be specified, the condition in the said subsection (1)(*b*)(ii) is not to be regarded as satisfied unless such further conditions as may be specified are also satisfied.

(3) The Minister may by regulations make such provision as he considers appropriate for the protection of data subjects in relation to the processing of personal data as to—

(*a*) the commission or alleged commission of any offence by data subjects,

(*b*) any proceedings for an offence committed or alleged to have been committed by data subjects, the disposal of such proceedings or the sentence of any court in such proceedings,

(*c*) any act or omission or alleged act or omission of data subjects giving rise to administrative sanctions,

(*d*) any civil proceedings in a court or other tribunal to which data subjects are parties or any judgment, order or decision of such a tribunal in any such proceedings,

and processing of personal data shall be in compliance with any regulations under this subsection.

56

(4) In this section—

'health professional' includes a registered medical practitioner, within the meaning of the Medical Practitioners Act 1978, a registered dentist, within the meaning of the Dentists Act 1985 or a member of any other class of health worker or social worker standing specified by regulations made by the Minister after consultation with the Minister for Health and Children and any other Minister of the Government who, having regard to his or her functions, ought, in the opinion of the Minister, to be consulted;

'medical purposes' includes the purposes of preventive medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.]

Annotations

Amendments:

F10 Inserted (1.07.2003) by *Data Protection Amendment Act 2003* (6/2003), s. 4, S.I. No. 207 of 2003. Amendments to section pursuant to 6/2003, s. 23 in respect of manual data held in relevant filing systems on the passing of 6/2003 commenced (24.10.2007) by s. 23(4), subject to transitional provision in subs. (5).

Modifications (not altering text):

C26 Term "registered medical practitioner" construed (3.7.2008) by *Medical Practitioners Act 2007* (25/2007), s. 108(1), S.I. No. 231 of 200.

Construction of references to registered medical practitioner and Medical Council, etc.

108.— (1) Every reference to a registered medical practitioner contained in any enactment or any statutory instrument shall be construed as a reference to a registered medical practitioner within the meaning of section 2.

...

Editorial Notes:

E13 Power pursuant to subs. (1)(b)(xi) exercised (15.06.2012) by *Data Protection Act 1988 (Section 2B) Regulations 2012* (S.I. No. 209 of 2012).

E14 Power pursuant to subs. (1)(b)(xi) exercised (27.09.2011) by *Data Protection Act 1988 (Section 2B) Regulations 2011* (S.I. No. 486 of 2011).

F11[Security measures for personal data.

2C.—(1) In determining appropriate security measures for the purposes of section 2(1)(*d*) of this Act, in particular (but without prejudice to the generality of that provision), where the processing involves the transmission of data over a network, a data controller—

(*a*) may have regard to the state of technological development and the cost of implementing the measures, and

(*b*) shall ensure that the measures provide a level of security appropriate to—

(i) the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, the data concerned, and

(ii) the nature of the data concerned.

(2) A data controller or data processor shall take all reasonable steps to ensure that—

57

(*a*) persons employed by him or her, and

(*b*) other persons at the place of work concerned,

are aware of and comply with the relevant security measures aforesaid.

(3) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall—

(*a*) ensure that the processing is carried out in pursuance of a contract in writing or in another equivalent form between the data controller and the data processor and that the contract provides that the data processor carries out the processing only on and subject to the instructions of the data controller and that the data processor complies with obligations equivalent to those imposed on the data controller by section 2(1)(*d*) of this Act,

(*b*) ensure that the data processor provides sufficient guarantees in respect of the technical security measures, and organisational measures, governing the processing, and

(*c*) take reasonable steps to ensure compliance with those measures.]

Annotations

Amendments:

F11 Inserted (1.07.2003) by *Data Protection Amendment Act 2003* (6/2003), s. 4, S.I. No. 207 of 2003.

Modifications (not altering text):

C27 Prospective affecting provision: section applied with modifications by *Criminal Justice (Forensic Evidence and DNA Database System) Act 2014* (11/2014), s. 123(1), (2)(c), not commenced as of date of revision.

Application of Act of 1988

123. (1) The Act of 1988 shall, with the modifications specified in subsection (2) and any other necessary modifications, apply to the processing of personal data supplied or received pursuant to—

(a) Chapter 2,

(b) Chapter 3, or

(c) an Article 7 request,

and, for the purposes of the foregoing application of the Act of 1988, references in it to that Act or the provisions of that Act shall, unless the context otherwise requires, be construed as including references to—

(i) Chapter 2 or the provisions of that Chapter,

(ii) Chapter 3 or the provisions of that Chapter, and

(iii) Chapter 3 of Part 5 of the Act of 2008 insofar as that Chapter applies to an Article 7 request or the provisions of that Chapter insofar as they apply to such a request.

(2) The modifications of the Act of 1988 referred to in subsection (1) are the following, namely—

...

(c) in section 2C, the substitution of the following subsection for subsection (1):

"(1) In determining appropriate security measures for the purposes of section 2(1)(d) (but without prejudice to the generality of that provision), a data controller—

(a) shall, in relation to the processing of personal data supplied or received pursuant to—

(i) Chapter 2 of Part 12 of the Act of 2014, or

58

(ii) Chapter 3 of that Part of that Act,

comply with the technical specifications of the automated search and comparison procedure required by the relevant European Union or international instrument, and

(b) shall ensure that the measures provide a level of security appropriate to—

(i) the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, or accidental alteration of, the data concerned, and

(ii) the nature of the data concerned.",

...

Editorial Notes:

E15 Prospective affecting provision: section applied to a deceased individual's relevant information as it does to a living individual's relevant information by *Health Identifiers Act 2014* (15/2014), s. 27(3), not commenced as of date of revision.

F12[Fair processing of personal data.

2D.—(1) Personal data shall not be treated, for the purposes of section 2(1)(*a*) of this Act, as processed fairly unless—

(*a*) in the case of data obtained from the data subject, the data controller ensures, so far as practicable, that the data subject has, is provided with, or has made readily available to him or her, at least the information specified in subsection (2) of this section,

(*b*) in any other case, the data controller ensures, so far as practicable, that the data subject has, is provided with, or has made readily available to him or her, at least the information specified in subsection (3) of this section—

(i) not later than the time when the data controller first processes the data, or

(ii) if disclosure of the data to a third party is envisaged, not later than the time of such disclosure.

(2) The information referred to in subsection (1)(*a*) of this section is:

(*a*) the identity of the data controller,

(*b*) if he or she has nominated a representative for the purposes of this Act, the identity of the representative,

(*c*) the purpose or purposes for which the data are intended to be processed, and

(*d*) any other information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data to be fair to the data subject such as information as to the recipients or categories of recipients of the data, as to whether replies to questions asked for the purpose of the collection of the data are obligatory, as to the possible consequences of failure to give such replies and as to the existence of the right of access to and the right to rectify the data concerning him or her.

(3) The information referred to in subsection (1)(*b*) of this section is:

(*a*) the information specified in subsection (2) of this section,

(*b*) the categories of data concerned, and

59

(*c*) the name of the original data controller.

(4) The said subsection (1)(*b*) does not apply—

(*a*) where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of the information specified therein proves impossible or would involve a disproportionate effort, or

(*b*) in any case where the processing of the information contained or to be contained in the data by the data controller is necessary for compliance with a legal obligation to which the data controller is subject other than an obligation imposed by contract,

if such conditions as may be specified in regulations made by the Minister after consultation with the Commissioner are complied with.]

Annotations

Amendments:

F12 Inserted (1.07.2003) by *Data Protection Amendment Act 2003* (6/2003), s. 4, S.I. No. 207 of 2003.

Right to establish existence of personal data.

3.—An individual who believes that a person keeps personal data shall, if he so requests the person in writing—

(*a*) be informed by the person whether he keeps any such data, and

(*b*) if he does, be given by the person a description of the data and the purposes for which they are kept,

as soon as may be and in any event not more than 21 days after the request has been given or sent to him.

Right of access.

4.—(1) F13[(*a*) Subject to the provisions of this Act, an individual shall, if he or she so requests a data controller by notice in writing—

(i) be informed by the data controller whether the data processed by or on behalf of the data controller include personal data relating to the individual,

(ii) if it does, be supplied by the data controller with a description of—

(I) the categories of data being processed by or on behalf of the data controller,

(II) the personal data constituting the data of which that individual is the data subject,

(III) the purpose or purposes of the processing, and

(IV) the recipients or categories of recipients to whom the data are or may be disclosed,

(iii) have communicated to him or her in intelligible form—

(I) the information constituting any personal data of which that individual is the data subject, and

(II) any information known or available to the data controller as to the source of those data unless the communication of that information is contrary to the public interest,

60

and

(iv) where the processing by automatic means of the data of which the individual is the data subject has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, be informed free of charge by the data controller of the logic involved in the processing,

as soon as may be and in any event not more than 40 days after compliance by the individual with the provisions of this section and, where any of the information is expressed in terms that are not intelligible to the average person without explanation, the information shall be accompanied by an explanation of those terms.

(*b*) A request under paragraph (*a*) of this subsection that does not relate to all of its subparagraphs shall, in the absence of any indication to the contrary, be treated as relating to all of them.]

(*c*) (i) A fee may be payable to the data controller concerned in respect of such a request as aforesaid and the amount thereof shall not exceed such amount as may be prescribed or an amount that in the opinion of the Commissioner is reasonable, having regard to the estimated cost to the data controller of compliance with the request, whichever is the lesser.

(ii) A fee paid by an individual to a data controller under *subparagraph (i)* of this paragraph shall be returned to him if his request is not complied with or the data controller rectifies or supplements, or erases part of, the data concerned (and thereby materially modifies the data) or erases all of the data on the application of the individual or in accordance with an enforcement notice or an order of a court.

(2) Where pursuant to provision made in that behalf under this Act there are separate entries in the register in respect of data kept by a data controller for different purposes, *subsection (1)* of this section shall apply as if it provided for the making of a separate request and the payment of a separate fee in respect of the data to which each entry relates.

(3) An individual making a request under this section shall supply the data controller concerned with such information as he may reasonably require in order to satisfy himself of the identity of the individual and to locate any relevant personal data or information.

(4) Nothing in *subsection (1)* of this section obliges a data controller to disclose to a data subject personal data relating to another individual unless that other individual has consented to the disclosure:

Provided that, where the circumstances are such that it would be reasonable for the data controller to conclude that, if any particulars identifying that other individual were omitted, the data could then be disclosed as aforesaid without his being thereby identified to the data subject, the data controller shall be obliged to disclose the data to the data subject with the omission of those particulars.

F14[(4A) (*a*) Where personal data relating to a data subject consist of an expression of opinion about the data subject by another person, the data may be disclosed to the data subject without obtaining the consent of that person to the disclosure.

(*b*) Paragraph (*a*) of this subsection does not apply—

(i) to personal data held by or on behalf of the person in charge of an institution referred to in section 5(1)(*c*) of this Act and consisting of an expression of opinion by another person about the data subject if the data subject is being or was detained in such an institution, or

61

(ii) if the expression of opinion referred to in that paragraph was given in confidence or on the understanding that it would be treated as confidential.]

(5) Information supplied pursuant to a request under *subsection (1)* of this section may take account of any amendment of the personal data concerned made since the receipt of the request by the data controller (being an amendment that would have been made irrespective of the receipt of the request) but not of any other amendment.

(6) (*a*) A request by an individual under *subsection (1)* of this section in relation to the results of an examination at which he was a candidate shall be deemed, for the purposes of this section, to be made on—

(i) the date of the first publication of the results of the examination, or

(ii) the date of the request,

whichever is the later; and *paragraph (a)* of the said *subsection (1)* shall be construed and have effect in relation to such a request as if for "40 days" there were substituted "60 days".

(*b*) In this subsection "examination" means any process for determining the knowledge, intelligence, skill or ability of a person by reference to his performance in any test, work or other activity.

(7) A notification of a refusal of a request made by an individual under and in compliance with the preceding provisions of this section shall be in writing and shall include a statement of the reasons for the refusal and an indication that the individual may complain to the Commissioner about the refusal.

(8) (*a*) If and whenever the Minister considers it desirable in the interests of data subjects F15[or in the public interest] to do so and by regulations so declares, the application of this section to personal data—

(i) relating to physical or mental health, or

(ii) kept for, or obtained in the course of, carrying out social work by a Minister of the Government, a local authority, a health board or a specified voluntary organisation or other body,

may be modified by the regulations in such manner, in such circumstances, subject to such safeguards and to such extent as may be specified therein.

(*b*) Regulations under *paragraph (a)* of this subsection shall be made only after consultation with the Minister for Health and any other Minister of the Government who, having regard to his functions, ought, in the opinion of the Minister, to be consulted and may make different provision in relation to data of different descriptions.

F16[(9) The obligations imposed by subsection (1)(*a*)(iii) (inserted by the Act of 2003) of this section shall be complied with by supplying the data subject with a copy of the information concerned in permanent form unless—

(*a*) the supply of such a copy is not possible or would involve disproportionate effort, or

(*b*) the data subject agrees otherwise.

(10) Where a data controller has previously complied with a request under subsection (1) of this section, the data controller is not obliged to comply with a subsequent identical or similar request under that subsection by the same individual unless, in the opinion of the data controller, a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(11) In determining for the purposes of subsection (10) of this section whether the reasonable interval specified in that subsection has elapsed, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

(12) Subsection (1)(*a*)(iv) of this section is not to be regarded as requiring the provision of information as to the logic involved in the taking of a decision if and to the extent only that such provision would adversely affect trade secrets or intellectual property (in particular any copyright protecting computer software).

F16[(13) (*a*) A person shall not, in connection with—

(i) the recruitment of another person as an employee,

(ii) the continued employment of another person, or

(iii) a contract for the provision of services to him or her by another person,

require that other person—

(I) to make a request under subsection (1) of this section, or

(II) to supply him or her with data relating to that other person obtained as a result of such a request.

(*b*) A person who contravenes paragraph (*a*) of this subsection shall be guilty of an offence.]]

Annotations

Amendments:

F13 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 5(a), S.I. No. 207 of 2003.

F14 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 5(b), S.I. No. 207 of 2003.

F15 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 5(c), S.I. No. 207 of 2003.

F16 Inserted (18.07.2014) by *Data Protection (Amendment) Act 2003* (6/2003), s. 5(d); subs. (13) S.I. No. 338 of 2014.

Modifications (not altering text):

C28 Prospective affecting provision: section applied with modifications by *Criminal Justice (Forensic Evidence and DNA Database System) Act 2014* (11/2014), s. 123(1), (2)(d), not commenced as of date of revision.

Application of Act of 1988

123. (1) The Act of 1988 shall, with the modifications specified in subsection (2) and any other necessary modifications, apply to the processing of personal data supplied or received pursuant to—

(a) Chapter 2,

(b) Chapter 3, or

(c) an Article 7 request,

and, for the purposes of the foregoing application of the Act of 1988, references in it to that Act or the provisions of that Act shall, unless the context otherwise requires, be construed as including references to—

(i) Chapter 2 or the provisions of that Chapter,

63

(ii) Chapter 3 or the provisions of that Chapter, and

(iii) Chapter 3 of Part 5 of the Act of 2008 insofar as that Chapter applies to an Article 7 request or the provisions of that Chapter insofar as they apply to such a request.

(2) The modifications of the Act of 1988 referred to in subsection (1) are the following, namely—

...

(d) in section 4, the addition of the following subsection:

"(14) Notwithstanding section 5, this section applies to the processing of personal data supplied or received pursuant to—

(a) Chapter 2 of Part 12 of the Act of 2014,

(b) Chapter 3 of that Part of that Act,

(c) an Article 7 request.",

...

C29 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C30 Application of section restricted (1.03.2013) by *Personal Insolvency Act 2012* (44/2012), s. 186, S.I. No. 63 of 2013.

Restriction of Data Protection Act 1988.

186.— Section 4 (as amended by section 5 of the Data Protection (Amendment) Act 2003) of the Data Protection Act 1988 shall not apply to data processed by—

(a) the Insolvency Service,

(b) an inspector appointed under section 176, or

(c) the Complaints Committee,

in the performance of functions assigned to those persons under this Act in so far as those functions relate to carrying out an investigation under this Part.

C31 Application of section restricted (6.07.2012) by *Property Services (Regulation) Act 2011* (40/2011), s. 93, S.I. No. 198 of 2012.

Restriction of Data Protection Act 1988.

93.— Section 4 (as amended by section 5 of the Data Protection (Amendment) Act 2003) of the Data Protection Act 1988 shall not apply to data processed by the Authority in the performance of its functions under this Act in so far as those functions relate to carrying out an investigation.

C32 Application of section restricted (18.07.2004) by *Commissions of Investigation Act 2004* (23/2004), s. 39, commenced on enactment.

Restriction of Data Protection Act 1988.

64

39.—Section 4 of the Data Protection Act 1988 does not apply to personal data provided to a commission for as long as the data is in the custody of—

(*a*) the commission,

(*b*) the specified Minister after being deposited with him or her under *section 43(2)*,

(*c*) a tribunal of inquiry after being made available to it under *section 45*, or

(*d*) a body after being transferred to it on the dissolution of a tribunal of inquiry to which the data was made available under *section 45*.

C33 Application of section restricted (16.12.2002) by *Residential Institutions Redress Act 2002* (13/2002), s. 30, S.I. No. 520 of 2005.

Restriction of Data Protection Act, 1988.

30.—Section 4 of the Data Protection Act, 1988 does not apply to personal data provided to the Board while the data is in the custody of the Board or the Review Committee.

C34 Application of section restricted (23.05.2000, establishment day) by *Commission to Inquire into Child Abuse Act 2000* (7/2000), s. 33, S.I. No. 149 of 2000.

Restriction of Data Protection Act. 1988.

33.—Section 4 of the Data Protection Act, 1988, does not apply to personal data provided to the Commission or a Committee while the data is in the custody of the Commission or a Committee, or in the case of such data provided to the Confidential Committee, of a body to which it is transferred by the Commission upon the dissolution of the Commission.

C35 Application of section restricted (19.04.1989) by *Data Protection (Access Modification) (Social Work) Regulations 1989* (S.I. No. 83 of 1989), reg. 4.

4. (1) Information constituting social work data shall not be supplied by or on behalf of a data controller to the data subject concerned in response to a request under section 4 (1) (*a*) of the Act if it would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject.

(2) Nothing in paragraph (1) of this Regulation excuses a data controller from supplying so much of the information sought by the request as can be supplied without causing the harm referred to in that paragraph.

(3) If the social work data include information supplied to a data controller by an individual (other than an employee or agent of the data controller) while carrying out social work, the data controller shall not supply that information to the data subject under section 4 (1) (*a*) of the Act without first consulting that individual.

C36 Application of section restricted (19.04.1989) by *Data Protection (Access Modification) (Health) Regulations 1989* (S.I. No. 82 of 1989), regs. 4-6.

4. (1) Information constituting health data shall not be supplied by or on behalf of a data controller to the data subject concerned in response to a request under section 4 (1) (*a*) of the Act if it would be likely to cause serious harm to the physical or mental health of the data subject.

(2) Nothing in paragraph (1) of this Regulation excuses a data controller from supplying so much of the information sought by the request as can be supplied without causing the harm referred to in that paragraph.

5. (1) A data controller who is not a health professional shall not—

(a) supply information constituting health data in response to a request under the said section 4 (1) (*a*), ...

(b) withhold any such information on the grounds specified in Regulation 4 (1) of these Regulations,

unless he has first consulted the person who appears to him to be the appropriate health professional.

65

6. Section 4 (4) of the Act shall not apply in relation to personal data relating to an individual other than the data controller or data subject concerned if that individual is a health professional who has been involved in the care of the data subject and the data relate to him in his capacity as such.

C37 Application of section restricted (19.04.1989) by *Data Protection Act 1988 (Restriction of Section 4) Regulations 1989* (S.I. No. 81 of 1989), reg. 3 and sch. *Adoption Act 1952* repealed (1.11.2010) by *Adoption Act 2010* (21/2010), s. 7(1) and sch. part 1, S.I. No. 511 of 2010.

3. The prohibition and restrictions on the disclosure, and the authorisations of the withholding, of information contained in the provision of the enactments specified in the Schedule to these Regulations shall prevail in the interests of the data subjects concerned and any other individuals concerned.

SCHEDULE

Section 22 (5) of the Adoption Act, 1952 (No. 25 of 1952).

Section 9 of the Ombudsman Act, 1980 (No. 26 of 1980).

Editorial Notes:

E16 Power pursuant to section exercised (19.04.1989) by *Data Protection (Access Modification) (Social Work) Regulations 1989* (S.I. No. 83 of 1989).

E16 Power pursuant to section exercised (19.04.1989) by *Data Protection (Access Modification) (Health) Regulations 1989* (S.I. No. 82 of 1989).

E18 Power pursuant to section exercised (16.12.1988) by *Data Protection (Fees) Regulations 1988* (S.I. No. 347 of 1988); regs. 5 and 6 revoked (4.04.1990) by *Data Protection (Fees) Regulations 1990* (S.I. No. 80 of 1990), reg. 5.

Restriction of right of access.

5.—(1) *Section 4* of this Act does not apply to personal data—

(*a*) kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of that section to the data would be likely to prejudice any of the matters aforesaid,

(*b*) to which, by virtue of *paragraph (a)* of this subsection, the said *section 4* does not apply and which are kept for the purpose of discharging a function conferred by or under any enactment and consisting of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in *paragraph (a)* of this subsection,

(*c*) in any case in which the application of that section would be likely to prejudice the security of, or the maintenance of good order and discipline in—

(i) a prison,

(ii) a place of detention provided under section 2 of the Prison Act, 1970,

(iii) a military prison or detention barrack within the meaning of the Defence Act, 1954, 1954, or

(iv) Saint Patrick's Institution,

(*d*) kept for the purpose of performing such functions conferred by or under any enactment as may be specified by regulations made by the Minister, being functions that, in the opinion of the Minister, are designed to protect members of the public against financial loss occasioned by—

66

(i) dishonesty, incompetence or malpractice on the part of persons concerned in the provision of banking, insurance, investment or other financial services or in the management of companies or similar organisations, or

(ii) the conduct of persons who have at any time been adjudicated bankrupt,

in any case in which the application of that section to the data would be likely to prejudice the proper performance of any of those functions,

(*e*) in respect of which the application of that section would be contrary to the interests of protecting the international relations of the State,

(*f*) consisting of an estimate of, or kept for the purpose of estimating, the amount of the liability of the data controller concerned on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of the section would be likely to prejudice the interests of the data controller in relation to the claim,

(*g*) in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his professional legal advisers or between those advisers,

F17[(*gg*) kept by the Commissioner or the Information Commissioner for the purposes of his or her functions,]

(*h*) kept only for the purpose of preparing statistics or carrying out research if the data are not used or disclosed (other than to a person to whom a disclosure of such data may be made in the circumstances specified in *section 8* of this Act) for any other purpose and the resulting statistics or the results of the research are not made available in a form that identifies any of the data subjects, or

(*i*) that are back-up data.

(2) Regulations under *subsections (1) (d)* and *(3) (b)* of this section shall be made only after consultation with any other Minister of the Government who, having regard to his functions, ought, in the opinion of the Minister, to be consulted.

(3) (*a*) Subject to *paragraph (b)* of this subsection, *section 4* of this Act, as modified by any other provisions thereof, shall apply notwithstanding any provision of or made under any enactment or rule of law that is in force immediately before the passing of this Act and prohibits or restricts the disclosure, or authorises the withholding, of information.

(*b*) If and whenever the Minister is of opinion that a prohibition, restriction or authorisation referred to in *paragraph (a)* of this subsection in relation to any information ought to prevail in the interests of the data subjects concerned or any other individuals and by regulations so declares, then, while the regulations are in force, the said *paragraph (a)* shall not apply as respects the provision or rule of law concerned and accordingly *section 4* of this Act, as modified as aforesaid, shall not apply in relation to that information.

Annotations

Amendments:

F17 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 6, S.I. No. 207 of 2003.

67

Editorial Notes:

E19 Power pursuant to subss. (1)(d) and (2) exercised (21.10.2009) by *Data Protection Act 1988 (Section 5(1)(d)) (Specification) Regulations 2009* (S.I. No. 421 of 2009).

E20 Power pursuant to subss. (1)(d) and (2) exercised (7.04.1993) by *Data Protection Act 1988 (Section 5(1)(d)) (Specification) Regulations 1993* (S.I. No. 95 of 1993).

E21 Power pursuant to subss. (2) and (3)(b) exercised (19.04.1989) by *Data Protection Act 1988 (Restriction of Section 4) Regulations 1989* (S.I. No. 81 of 1989).

E22 Previous affecting provision: power pursuant to subss. (1)(d) and (2) exercised (19.04.1989) by *Data Protection Act 1988 (Section 5(1)(d)) (Specification) Regulations 1989* (S.I. No. 84 of 1989); revoked (7.04.1993) by *Data Protection Act 1988 (Section 5(1)(d) (Specification) Regulations 1993* (S.I. No. 95 of 1993), reg. 4.

Right of rectification or erasure.

6.—(1) An individual shall, if he so requests in writing a data controller who keeps personal data relating to him, be entitled to have rectified or, where appropriate, F18[blocked or] erased any such data in relation to which there has been a contravention by the data controller of *section 2 (1)* of this Act; and the data controller shall comply with the request as soon as may be and in any event not more than 40 days after it has been given or sent to him:

Provided that the data controller shall, as respects data that are inaccurate or not kept up to date, be deemed—

(*a*) to have complied with the request if he supplements the data with a statement (to the terms of which the individual has assented) relating to the matters dealt with by the data, and

(*b*) if he supplements the data as aforesaid, not to be in contravention of *paragraph (b)* of the said *section 2 (1)*.

F19[(2) Where a data controller complies, or is deemed to have complied, with a request under subsection (1) of this section, he or she shall, as soon as may be and in any event not more than 40 days after the request has been given or sent to him or her, notify—

(*a*) the individual making the request, and

(*b*) if such compliance materially modifies the data concerned, any person to whom the data were disclosed during the period of 12 months immediately before the giving or sending of the request unless such notification proves impossible or involves a disproportionate effort,]

Annotations

Amendments:

F18 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 7(a), S.I. No. 207 of 2003.

F19 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 7(b), S.I. No. 207 of 2003; subs. (2)(b) commenced (18.07.2014) by S.I. No. 338 of 2014.

Modifications (not altering text):

C38 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

68

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

F20[Right of data subject to object to processing likely to cause damage or distress.

6A.—(1) Subject to subsection (3) and unless otherwise provided by any enactment, an individual is entitled at any time, by notice in writing served on a data controller, to request him or her to cease within a reasonable time, or not to begin, processing or processing for a specified purpose or in a specified manner any personal data in respect of which he or she is the data subject if the processing falls within subsection (2) of this section on the ground that, for specified reasons—

(*a*) the processing of those data or their processing for that purpose or in that manner is causing or likely to cause substantial damage or distress to him or her or to another person, and

(*b*) the damage or distress is or would be unwarranted.

(2) This subsection applies to processing that is necessary—

(*a*) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the data are or are to be disclosed, or

(*b*) for the purposes of the legitimate interests pursued by the data controller to whom the data are or are to be disclosed, unless those interests are overridden by the interests of the data subject in relation to fundamental rights and freedoms and, in particular, his or her right to privacy with respect to the processing of personal data.

(3) Subsection (1) does not apply—

(*a*) in a case where the data subject has given his or her explicit consent to the processing,

(*b*) if the processing is necessary—

(i) for the performance of a contract to which the data subject is a party,

(ii) in order to take steps at the request of the data subject prior to his or her entering into a contract,

(iii) for compliance with any legal obligation to which the data controller or data subject is subject other than one imposed by contract, or

(iv) to protect the vital interests of the data subject,

(*c*) to processing carried out by political parties or candidates for election to, or holders of elective political office, in the course of electoral activities, or

(*d*) in such other cases, if any, as may be specified in regulations made by the Minister after consultation with the Commissioner.

69

(4) Where a notice under subsection (1) of this section is served on a data controller, he or she shall, as soon as practicable and in any event not later than 20 days after the receipt of the notice, serve a notice on the individual concerned—

(*a*) stating that he or she has complied or intends to comply with the request concerned, or

(*b*) stating that he or she is of opinion that the request is unjustified to any extent and the reasons for the opinion and the extent (if any) to which he or she has complied or intends to comply with it.

(5) If the Commissioner is satisfied, on the application to him or her in that behalf of an individual who has served a notice under subsection (1) of this section that appears to the Commissioner to be justified, or to be justified to any extent, that the data controller concerned has failed to comply with the notice or to comply with it to that extent and that not less than 40 days have elapsed since the receipt of the notice by him or her, the Commissioner may, by an enforcement notice served on the data controller, order him or her to take such steps for complying with the request, or for complying with it to that extent, as the Commissioner thinks fit and specifies in the enforcement notice, and that notice shall specify the reasons for the Commissioner being satisfied as aforesaid.]

Annotations

Amendments:

F20 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 8, S.I. No. 207 of 2003.

F21[Rights in relation to automated decision taking.

6B.—(1) Subject to subsection (2) of this section, a decision which produces legal effects concerning a data subject or otherwise significantly affects a data subject may not be based solely on processing by automatic means of personal data in respect of which he or she is the data subject and which is intended to evaluate certain personal matters relating to him or her such as, for example (but without prejudice to the generality of the foregoing), his or her performance at work, creditworthiness, reliability or conduct.

(2) Subsection (1) of this section does not apply—

(*a*) in a case in which a decision referred to in that subsection—

(i) is made in the course of steps taken—

(I) for the purpose of considering whether to enter into a contract with the data subject,

(II) with a view to entering into such a contract, or

(III) in the course of performing such a contract,

or

(ii) is authorised or required by any enactment and the data subject has been informed of the proposal to make the decision, and

(iii) either—

(I) the effect of the decision is to grant a request of the data subject, or

(II) adequate steps have been taken to safeguard the legitimate interests of the data subject by, for example (but without prejudice to the generality of the foregoing), the making of arrangements to enable

70

him or her to make representations to the data controller in relation to the proposal,

or

(*b*) if the data subject consents to the processing referred to in subsection (1).]

Annotations

Amendments:

F21 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 8, S.I. No. 207 of 2003.

Duty of care owed by data controllers and data processors.

7.—For the purposes of the law of torts and to the extent that that law does not so provide, a person, being a data controller or a data processor, shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned:

Provided that, for the purposes only of this section, a data controller shall be deemed to have complied with the provisions of *section 2 (1) (b)* of this Act if and so long as the personal data concerned accurately record data or other information received or obtained by him from the data subject or a third party and include (and, if the data are disclosed, the disclosure is accompanied by)—

(*a*) an indication that the information constituting the data was received or obtained as aforesaid,

(*b*) if appropriate, an indication that the data subject has informed the data controller that he regards the information as inaccurate or not kept up to date, and

(*c*) any statement with which, pursuant to this Act, the data are supplemented.

Annotations

Modifications (not altering text):

C39 Prospective affecting provision: section applied with modifications by *Criminal Justice (Forensic Evidence and DNA Database System) Act 2014* (11/2014), s. 123(1), (2)(e), not commenced as of date of revision.

Application of Act of 1988

123. (1) The Act of 1988 shall, with the modifications specified in subsection (2) and any other necessary modifications, apply to the processing of personal data supplied or received pursuant to—

(a) Chapter 2,

(b) Chapter 3, or

(c) an Article 7 request,

and, for the purposes of the foregoing application of the Act of 1988, references in it to that Act or the provisions of that Act shall, unless the context otherwise requires, be construed as including references to—

(i) Chapter 2 or the provisions of that Chapter,

(ii) Chapter 3 or the provisions of that Chapter, and

(iii) Chapter 3 of Part 5 of the Act of 2008 insofar as that Chapter applies to an Article 7 request or the provisions of that Chapter insofar as they apply to such a request.

71

(2) The modifications of the Act of 1988 referred to in subsection (1) are the following, namely—

...

(e) in section 7—

(i) the proviso shall not apply to a data controller in respect of personal data received or obtained by him or her from a body in a designated state pursuant to a European Union or international instrument,

(ii) the designation of the section (as modified by subparagraph (i)) as subsection (1) of that section, and

(iii) the addition of the following subsections:

"(2) A data controller shall not use the inaccuracy of personal data received by him or her from a body in a designated state pursuant to a European Union or international instrument as a ground to avoid or reduce his or her liability to the data subject concerned under subsection (1).

(3) Where—

(a) the Minister or the Commissioner of the Garda Síochána pays damages to a data subject under this section for damage caused to the data subject by reason of inaccurate data received by the national contact point in relation to DNA data or the national contact point in relation to dactyloscopic data, as may be appropriate, from a body in a designated state pursuant to Chapter 2 or 3 of Part 12 of the Act of 2014, or

(b) the Minister, the Commissioner of the Garda Síochána or the Director of Public Prosecutions pays damages to a data subject under this section for damage caused to the data subject by reason of inaccurate data received by the Central Authority, the Garda Síochána or the Director of Public Prosecutions, as may be appropriate, from a body in a Member State or Iceland or Norway pursuant to an Article 7 request,

the Minister, the Commissioner of the Garda Síochána or the Director of Public Prosecutions, as the case may be, may seek a refund of the amount that he or she paid in damages to the data subject concerned from the body in the designated state concerned.

(4) Where—

(a) a body in a designated state applies to the national contact point in relation to DNA data or the national contact point in relation to dactyloscopic data for a refund of damages paid by it, or on its behalf, on foot of a decision or finding of a court or other tribunal or the data protection authority in that designated state for damage caused to a data subject by reason of inaccurate data sent by the national contact point concerned to that body pursuant to Chapter 2 or 3 of Part 12 of the Act of 2014, or

(b) a body in a Member State or Iceland or Norway applies to the Minister or the Director of Public Prosecutions for a refund of damages paid by it, or on its behalf, on foot of a decision or finding of a court or other tribunal or the data protection authority in that Member State or Iceland or Norway, as the case may be, for damage caused to a data subject by reason of inaccurate data sent by the Minister or the Director of Public Prosecutions, as the case may be, to that body pursuant to an Article 7 request,

the Minister or the Commissioner of the Garda Síochána, as may be appropriate, in the circumstances referred to in paragraph (a), or the Minister or the Director of Public Prosecutions, as may be appropriate, in the circumstances referred to in paragraph (b), shall refund to the body in the designated state concerned the amount paid in damages by it, or on its behalf, to the data subject concerned.",

...

72

Disclosure of personal data in certain cases.

8.—Any restrictions in this Act on the F22[processing] of personal data do not apply if the F22[processing] is—

(*a*) in the opinion of a member of the Garda Síochána not below the rank of chief superintendent or an officer of the Permanent Defence Force who holds an army rank not below that of colonel and is designated by the Minister for Defence under this paragraph, required for the purpose of safeguarding the security of the State,

(*b*) required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid,

(*c*) required in the interests of protecting the international relations of the State,

(*d*) required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property,

(*e*) required by or under any enactment or by a rule of law or order of a court,

(*f*) required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the F22[processing] is a party or a witness,

(*g*) F23[...]

(*h*) made at the request or with the consent of the data subject or a person acting on his behalf.

Annotations

Amendments:

F22 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 9(a), S.I. No. 207 of 2003.

F23 Deleted(1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 9(b), S.I. No. 207 of 2003.

Modifications (not altering text):

C40 Prospective affecting provision: section applied with modifications by *Criminal Justice (Forensic Evidence and DNA Database System) Act 2014* (11/2014), s. 123(1), (2)(f), not commenced as of date of revision.

Application of Act of 1988

123. (1) The Act of 1988 shall, with the modifications specified in subsection (2) and any other necessary modifications, apply to the processing of personal data supplied or received pursuant to—

(a) Chapter 2,

(b) Chapter 3, or

(c) an Article 7 request,

and, for the purposes of the foregoing application of the Act of 1988, references in it to that Act or the provisions of that Act shall, unless the context otherwise requires, be construed as including references to—

(i) Chapter 2 or the provisions of that Chapter,

(ii) Chapter 3 or the provisions of that Chapter, and

73

(iii) Chapter 3 of Part 5 of the Act of 2008 insofar as that Chapter applies to an Article 7 request or the provisions of that Chapter insofar as they apply to such a request.

(2) The modifications of the Act of 1988 referred to in subsection (1) are the following, namely—

...

(f) section 8(b) —

(i) insofar as it relates to the purpose of detecting or investigating offences, shall not apply to the processing of data pursuant to Chapter 2,

(ii) insofar as it relates to the purpose of preventing, detecting or investigating offences, shall not apply to the processing of personal data pursuant to Chapter 3, or

(iii) insofar as it relates to the purpose of detecting or investigating offences or apprehending or prosecuting offenders, shall not apply to the processing of personal data pursuant to an Article 7 request,

which are or have been supplied by or to a data controller in the State pursuant to a European Union or international instrument, and

...

The Data Protection Commissioner

The Commissioner.

9.—(1) For the purposes of this Act, there shall be a person (referred to in this Act as the Commissioner) who shall be known as an Coimisinéir Cosanta Sonraí or, in the English language, the Data Protection Commissioner; the Commissioner shall perform the functions conferred on him by this Act.

F24[(1A) (*a*) The lawfulness of the processing of personal data (including their transmission to the Central Unit of Eurodac established pursuant to the Council Regulation) in accordance with the Council Regulation shall be monitored by the Commissioner.

(*b*) In paragraph (*a*) of this subsection, 'the Council Regulation' means Council Regulation (EC) No. 2725/2000 of 11 December 2000[2] concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention.

(1B) The Commissioner shall arrange for the dissemination in such form and manner as he or she considers appropriate of—

(*a*) any Community finding (within the meaning of subsection (2)(*b*) (inserted by the *Act of 2003*) of section 11 of this Act),

(*b*) any decision of the European Commission or the European Council under the procedure provided for in Article 31(2) of the Directive that is made for the purposes of paragraph 3 or 4 of Article 26 of the Directive, and

(*c*) such other information as may appear to him or her to be expedient to give to data controllers in relation to the protection of the rights and freedoms of data subjects in respect of the processing of personal data in countries and territories outside the European Economic Area.

(1C) The Commissioner shall be the supervisory authority in the State for the purposes of the Directive.

(1D) The Commissioner shall also perform any functions in relation to data protection that the Minister may confer on him or her by regulations for the purpose of enabling the Government to give effect to any international obligations of the State.]

(2) The provisions of the *Second Schedule* to this Act shall have effect in relation to the Commissioner.

[2] O.J. No. L 316, 15.12.00, p. 0001-0010.

74

F25[(3) The Commissioner shall be the supervisory authority in the State for the purposes of Articles 4, 17, 25 and 26 of the Directive.]

Annotations

Amendments:

F24 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 10, S.I. No. 207 of 2003.

F25 Inserted (1.04.2002) by *European Communities (Data Protection) Regulations 2001* (S.I. No. 626 of 2001), reg. 4.

Modifications (not altering text):

C41 Prospective affecting provision: section applied with modifications by *Criminal Justice (Forensic Evidence and DNA Database System) Act 2014* (11/2014), s. 123(1), (2)(g), not commenced as of date of revision.

Application of Act of 1988

123. (1) The Act of 1988 shall, with the modifications specified in subsection (2) and any other necessary modifications, apply to the processing of personal data supplied or received pursuant to—

(a) Chapter 2,

(b) Chapter 3, or

(c) an Article 7 request,

and, for the purposes of the foregoing application of the Act of 1988, references in it to that Act or the provisions of that Act shall, unless the context otherwise requires, be construed as including references to—

(i) Chapter 2 or the provisions of that Chapter,

(ii) Chapter 3 or the provisions of that Chapter, and

(iii) Chapter 3 of Part 5 of the Act of 2008 insofar as that Chapter applies to an Article 7 request or the provisions of that Chapter insofar as they apply to such a request.

(2) The modifications of the Act of 1988 referred to in subsection (1) are the following, namely—

...

(g) in section 9, the insertion of the following subsection after subsection (1D):

"(1E) (a) The Commissioner shall be the competent data protection authority in the State for the purposes of a European Union or international instrument.

(b) The lawfulness of the processing of personal data supplied or received pursuant to—

(i) Chapter 2 of Part 12 of the Act of 2014,

(ii) Chapter 3 of that Part of that Act, and

(iii) an Article 7 request,

shall be monitored by the Commissioner.

(c) The performance by the Commissioner of his or her function under paragraph (b) shall include the carrying out of random checks on the processing of personal data referred to in that paragraph.

(d) The Commissioner may request the data protection authority of a designated state to perform its functions under the law of that designated state with regard to checking the lawfulness of the processing of personal data supplied by the State to that designated state pursuant to the relevant European Union or international instrument.

75

(e) The Commissioner may receive information from the data protection authority of a designated state arising from the performance by it of the functions referred to in paragraph (d) with regard to the processing of the personal data concerned.

(f) The Commissioner shall, at the request of the data protection authority of a designated state, perform his or her functions under paragraphs (a) to (c) of this subsection and he or she shall furnish information to that authority with regard to the processing of the personal data the subject of the request.".

C42 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

Editorial Notes:

E23 Power pursuant to section exercised (25.05.1993) by *Data Protection Commissioner Superannuation Scheme 1993* (S.I. No. 141 of 1993).

Enforcement of data protection.

10.—(1) (*a*) The Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened F26[...] in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.

(*b*) Where a complaint is made to the Commissioner under *paragraph (a)* of this subsection, the Commissioner shall—

(i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious, and

F27[(ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it to the Court under section 26 of this Act within 21 days from the receipt by him or her of the notification.]

F28[(1A) The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and to identify any contravention thereof.]

(2) If the Commissioner is of opinion that a person F29[...] has contravened or is contravening a provision of this Act (other than a provision the contravention of which is an offence), the Commissioner may, by notice in writing (referred to in this Act as an enforcement notice) served on the person, require him to take such steps as are

76

specified in the notice within such time as may be so specified to comply with the provision concerned.

(3) Without prejudice to the generality of *subsection (2)* of this section, if the Commissioner is of opinion that a data controller has contravened *section 2 (1)* of this Act, the relevant enforcement notice may require him—

F27[(*a*) to block, rectify, erase or destroy any of the data concerned, or]

(*b*) to supplement the data with such statement relating to the matters dealt with by them as the Commissioner may approve of; and as respects data that are inaccurate or not kept up to date, if he supplements them as aforesaid, he shall be deemed not to be in contravention of *paragraph (b)* of the said *section 2 (1)*.

(4) An enforcement notice shall—

(*a*) specify any provision of this Act that, in the opinion of the Commissioner, has been or is being contravened and the reasons for his having formed that opinion, and

(*b*) subject to *subsection (6)* of this section, state that the person concerned may appeal to the Court under *section 26* of this Act against the requirement specified in the notice within 21 days from the service of the notice on him.

(5) Subject to *subsection (6)* of this section, the time specified in an enforcement notice for compliance with a requirement specified therein shall not be expressed to expire before the end of the period of 21 days specified in *subsection (4) (b)* of this section and, if an appeal is brought against the requirement, the requirement need not be complied with and *subsection (9)* of this section shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(6) If the Commissioner—

(*a*) by reason of special circumstances, is of opinion that a requirement specified in an enforcement notice should be complied with urgently, and

(*b*) includes a statement to that effect in the notice,

subsections (4) (b) and *(5)* of this section shall not apply in relation to the notice, but the notice shall contain a statement of the effect of the provisions of *section 26* (other than *subsection (3)*) of this Act and shall not require compliance with the requirement before the end of the period of 7 days beginning on the date on which the notice is served.

(7) On compliance by a data controller with a requirement under *subsection (3)* of this section, he shall, as soon as may be and in any event not more than 40 days after such compliance, notify—

(*a*) the data subject concerned, and

F27[(*b*) if such compliance materially modifies the data concerned, any person to whom the data were disclosed during the period beginning 12 months before the date of the service of the enforcement notice concerned and ending immediately before such compliance unless such notification proves impossible or involves a disproportionate effort,

of the blocking, rectification, erasure, destruction or statement concerned.]

(8) The Commissioner may cancel an enforcement notice and, if he does so, shall notify in writing the person on whom it was served accordingly.

(9) A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an enforcement notice shall be guilty of an offence.

77

Annotations

Amendments:

F26 Deleted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 11(a)(i), S.I. No. 207 of 2003.

F27 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 11(a)(ii), (d) and (e), S.I. No. 207 of 2003; subs. (7)(b), substituted by s. 11(e), commenced (18.07.2014) by S.I. No. 337 of 2014.

F28 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 11(b), S.I. No. 207 of 2003.

F29 Deleted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 11(c), S.I. No. 207 of 2003.

Modifications (not altering text):

C43 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C44 Application of section extended with any necessary modifications (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

Unsolicited commercial communications.

9. ...

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

...

(9) Section 10 of the Act applies as if —

78

(a) in subsection (1)(a), "in relation to a person either where the person complains" were substituted for "by a data controller or a data processor in relation to an individual either where the individual complains",

(b) in subsection (1)(b), the following subparagraph were substituted for subparagraph (ii):

"(ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, notify in writing the person who made the complaint of his or her decision in relation to it and that the person may, if aggrieved by the decision, appeal against it to the Court under section 26 of this Act within 21 days from the receipt by the person of the notification.",

(c) the following subsection were inserted after subsection (1):

"(1A) The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with Regulation 9 of the Regulations of 2003 and to identify any contravention thereof.",

(d) in subsection (2), there were deleted, "being a data controller or a data processor,",

(e) in subsection (3), there were substituted the following paragraph for paragraph (a):

"(a) to block, rectify, erase or destroy any of the data concerned, or", and ,

(f) in subsection (7), there were substituted the following for so much of the subsection as follows paragraph (a):

"(b) if such compliance materially modifies the data concerned, any person to whom the data were disclosed during the previous 12 months before the date of the service of the enforcement notice concerned and ending immediately before such compliance unless such notification proves impossible or involves a disproportionate effort,

of the blocking, rectification, erasure, destruction or statement concerned.".

...

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

Editorial Notes:

E24 Previous affecting provision: subs. 7(b) as enacted not commenced; substituted as per F-Note above.

E25 Previous affecting provision: application of section extended (from the date on which the declaration by the State under Article 32 (4) of the Customs Co-operation Convention took effect to 24 October 2007) by *Customs and Excise (Mutual Assistance) Act 2001 (Section 8) (Protection of Manual Data) Regulations 2004* (S.I. No. 254 of 2004), reg. 10(2).

E26 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35, subject to transitional provisions in reg. 34.

E27 Previous affecting provision: non-textual amendments identical to those made by *Data Protection (Amendment) Act 2003* above were made by the *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(9).

79

E28 Previous affecting provision: application of ss. 10, 12, 24, 25, 26 (insofar as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Commissioner in relation to a complaint under section 10(1)(a)) and ss. 27 to 31 extended with any necessary modifications (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 12; revoked (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 24.

Prohibition on transfer of personal data outside State.

F30[**11.**—(1) The transfer of personal data to a country or territory outside the European Economic Area may not take place unless that country or territory ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding the transfer and, in particular, but without prejudice to the generality of the foregoing, to—

(*a*) the nature of the data,

(*b*) the purposes for which and the period during which the data are intended to be processed,

(*c*) the country or territory of origin of the information contained in the data,

(*d*) the country or territory of final destination of that information,

(*e*) the law in force in the country or territory referred to in paragraph (*d*),

(*f*) any relevant codes of conduct or other rules which are enforceable in that country or territory,

(*g*) any security measures taken in respect of the data in that country or territory, and

(*h*) the international obligations of that country or territory.

(2) (*a*) Where in any proceedings under this Act a question arises—

(i) whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area to which personal data are to be transferred, and

(ii) a Community finding has been made in relation to transfers of the kind in question,

the question shall be determined in accordance with that finding.

(*b*) In paragraph (*a*) of this subsection 'Community finding' means a finding of the European Commission made for the purposes of paragraph (4) or (6) of Article 25 of the Directive under the procedure provided for in Article 31(2) of the Directive in relation to whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area.

(3) The Commissioner shall inform the Commission and the supervisory authorities of the other Member States of any case where he or she considers that a country or territory outside the European Economic Area does not ensure the adequate level of protection referred to in subsection (1) of this section.

(4) (*a*) This section shall not apply to a transfer of data if—

(i) the transfer of the data or the information constituting the data is required or authorised by or under—

(I) any enactment, or

80

(II) any convention or other instrument imposing an international obligation on the State,

(ii) the data subject has given his or her consent to the transfer,

(iii) the transfer is necessary—

(I) for the performance of a contract between the data subject and the data controller, or

(II) for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller,

(iv) the transfer is necessary—

(I) for the conclusion of a contract between the data controller and a person other than the data subject that—

(A) is entered into at the request of the data subject, and

(B) is in the interests of the data subject, or

(II) for the performance of such a contract,

(v) the transfer is necessary for reasons of substantial public interest,

(vi) the transfer is necessary for the purpose of obtaining legal advice or for the purpose of or in connection with legal proceedings or prospective legal proceedings or is otherwise necessary for the purposes of establishing or defending legal rights,

(vii) the transfer is necessary in order to prevent injury or other damage to the health of the data subject or serious loss of or damage to property of the data subject or otherwise to protect his or her vital interests, and informing the data subject of, or seeking his or her consent to, the transfer is likely to damage his or her vital interests,

(viii) the transfer is of part only of the personal data on a register established by or under an enactment, being—

(I) a register intended for consultation by the public, or

(II) a register intended for consultation by persons having a legitimate interest in its subject matter,

and, in the case of a register referred to in clause (II) of this subparagraph, the transfer is made, at the request of, or to, a person referred to in that clause and any conditions to which such consultation is subject are complied with by any person to whom the data are or are to be transferred, or

(ix) the transfer has been authorised by the Commissioner where the data controller adduces adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals and for the exercise by individuals of their relevant rights under this Act or the transfer is made on terms of a kind approved by the Commissioner as ensuring such safeguards.

(*b*) The Commissioner shall inform the European Commission and the supervisory authorities of the other states in the European Economic Area of any authorisation or approval under paragraph (*a*)(ix) of this subsection.

(*c*) The Commissioner shall comply with any decision of the European Commission under the procedure laid down in Article 31.2 of the Directive made for the purposes of paragraph 3 or 4 of Article 26 of the Directive.

81

(5) The Minister may, after consultation with the Commissioner, by regulations specify—

(*a*) the circumstances in which a transfer of data is to be taken for the purposes of subsection (4)(*a*)(v) of this section to be necessary for reasons of substantial public interest, and

(*b*) the circumstances in which such a transfer which is not required by or under an enactment is not to be so taken.

(6) Where, in relation to a transfer of data to a country or territory outside the European Economic Area, a data controller adduces the safeguards for the data subject concerned referred to in subsection (4)(*a*)(ix) of this section by means of a contract embodying the contractual clauses referred to in paragraph 2 or 4 of Article 26 of the Directive, the data subject shall have the same right—

(*a*) to enforce a clause of the contract conferring rights on him or her or relating to such rights, and

(*b*) to compensation or damages for breach of such a clause,

that he or she would have if he or she were a party to the contract.

(7) The Commissioner may, subject to the provisions of this section, prohibit the transfer of personal data from the State to a place outside the State unless such transfer is required or authorised by or under any enactment or required by any convention or other instrument imposing an international obligation on the State.

(8) In determining whether to prohibit a transfer of personal data under this section, the Commissioner shall also consider whether the transfer would be likely to cause damage or distress to any person and have regard to the desirability of facilitating international transfers of data.

(9) A prohibition under subsection (7) of this section shall be effected by the service of a notice (referred to in this Act as a prohibition notice) on the person proposing to transfer the data concerned.

(10) A prohibition notice shall—

(*a*) prohibit the transfer concerned either absolutely or until the person aforesaid has taken such steps as are specified in the notice for protecting the interests of the data subjects concerned,

(*b*) specify the time when it is to take effect,

(*c*) specify the grounds for the prohibition, and

(*d*) subject to subsection (12) of this section, state that the person concerned may appeal to the Court under section 26 of this Act against the prohibition specified in the notice within 21 days from the service of the notice on him or her.

(11) Subject to subsection (12) of this section, the time specified in a prohibition notice for compliance with the prohibition specified therein shall not be expressed to expire before the end of the period of 21 days specified in subsection (10)(*d*) of this section and, if an appeal is brought against the prohibition, the prohibition need not be complied with and subsection (15) of this section shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(12) If the Commissioner—

(*a*) by reason of special circumstances, is of opinion that a prohibition specified in a prohibition notice should be complied with urgently, and

(*b*) includes a statement to that effect in the notice,

82

subsections (10)(*d*) and (11) of this section shall not apply in relation to the notice but the notice shall contain a statement of the effect of the provisions of section 26 (other than subsection (3)) of this Act and shall not require compliance with the prohibition before the end of the period of 7 days beginning on the date on which the notice is served.

(13) The Commissioner may cancel a prohibition notice and, if he or she does so, shall notify in writing the person on whom it was served accordingly.

(14) (*a*) This section applies, with any necessary modifications, to a transfer of information from the State to a place outside the State for conversion into personal data as it applies to a transfer of personal data from the State to such a place.

(*b*) In paragraph (*a*) of this subsection 'information' means information (not being data) relating to a living individual who can be identified from it.

(15) A person who, without reasonable excuse, fails or refuses to comply with a prohibition specified in a prohibition notice shall be guilty of an offence.]

Annotations

Amendments:

F30 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 12, S.I. No. 207 of 2003.

Editorial Notes:

E29 Previous affecting provision: section substituted (1.04.2002) by *European Communities (Data Protection) Regulations 2001* (S.I. No. 626 of 2001), reg. 5; substituted as per F-note above.

Power to require information.

12.—(1) The Commissioner may, by notice in writing (referred to in this Act as an information notice) served on a person, require the person to furnish to him in writing within such time as may be specified in the notice such information in relation to matters specified in the notice as is necessary or expedient for the performance by the Commissioner of his functions.

(2) Subject to *subsection (3)* of this section—

(*a*) an information notice shall state that the person concerned may appeal to the Court under *section 26* of this Act against the requirement specified in the notice within 21 days from the service of the notice on him, and

(*b*) the time specified in the notice for compliance with a requirement specified therein shall not be expressed to expire before the end of the period of 21 days specified in *paragraph (a)* of this subsection and, if an appeal is brought against the requirement, the requirement need not be complied with and *subsection (5)* of this section shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(3) If the Commissioner—

(*a*) by reason of special circumstances, is of opinion that a requirement specified in an information notice should be complied with urgently, and

(*b*) includes a statement to that effect in the notice,

subsection (2) of this section shall not apply in relation to the notice, but the notice shall contain a statement of the effect of the provisions of *section 26* (other than *subsection (3)*) of this Act and shall not require compliance with the requirement

83

before the end of the period of 7 days beginning on the date on which the notice is served.

(4) (*a*) No enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing to the Commissioner any information that is necessary or expedient for the performance by the Commissioner of his functions.

(*b*) *Paragraph (a)* of this subsection does not apply to information that in the opinion of the Minister or the Minister for Defence is, or at any time was, kept for the purpose of safeguarding the security of the State or information that is privileged from disclosure in proceedings in any court.

(5) A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an information notice or who in purported compliance with such a requirement furnishes information to the Commissioner that the person knows to be false or misleading in a material respect shall be guilty of an offence.

Annotations

Modifications (not altering text):

C45 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C46 Application of section extended with any necessary modifications (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

Unsolicited commercial communications.

9. ...

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

...

84

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

Editorial Notes:

E30 Previous affecting provision: section applied to extend performance of Commissioner's functions (from the date on which the declaration by the State under Article 32 (4) of the Customs Co-operation Convention took effect to 24 October 2007) by *Customs and Excise (Mutual Assistance) Act 2001 (Section 8) (Protection of Manual Data) Regulations 2004* (S.I. No. 254 of 2004), reg. 10(3).

E31 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35 subject to transitional provisions in reg. 34.

E32 Previous affecting provision: application of ss. 10, 12, 24, 25, 26 (insofar as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Commissioner in relation to a complaint under section 10(1)(a)) and ss. 27 to 31 extended with any necessary modifications (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 12; revoked (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 24.

F31[Prior checking of processing by Commissioner.

12A.—(1) This section applies to any processing that is of a prescribed description, being processing that appears to the Commissioner to be particularly likely—

(*a*) to cause substantial damage or substantial distress to data subjects, or

(*b*) otherwise significantly to prejudice the rights and freedoms of data subjects.

(2) The Commissioner, on receiving—

(*a*) an application under section 17 of this Act by a person to whom section 16 of this Act applies for registration in the register and any prescribed information and any other information that he or she may require, or

(*b*) a request from a data controller in that behalf,

shall consider and determine—

(i) whether any of the processing to which the application or request relates is processing to which this section applies,

(ii) if it does, whether the processing to which this section applies is likely to comply with the provisions of this Act.

(3) Subject to subsection (4) of this section, the Commissioner shall, within the period of 90 days from the day on which he or she receives an application or a request referred to in subsection (2) of this section, serve a notice on the data controller concerned stating the extent to which, in the opinion of the Commissioner, the proposed processing is likely or unlikely to comply with the provisions of this Act.

(4) Before the end of the period referred to in subsection (3), the Commissioner may, by reason of special circumstances, extend that period once only, by notice in writing served on the data controller concerned, by such further period not exceeding 90 days as the Commissioner may specify in the notice.

85

(5) If, for the purposes of his or her functions under this section, the Commissioner serves an information notice on the data controller concerned before the end of the period referred to in subsection (3) of this section or that period as extended under subsection (4) of this section—

(*a*) the period from the date of service of the notice to the date of compliance with the requirement in the notice, or

(*b*) if the requirement is set aside under section 26 of this Act, the period from the date of such service to the date of such setting aside,

shall be added to the period referred to in the said subsection (3) or that period as so extended as aforesaid.

(6) Processing to which this section applies shall not be carried on unless—

(*a*) the data controller has—

(i) previously made an application under section 17 of this Act and furnished the information specified in that section to the Commissioner, or

(ii) made a request under subsection (2) of this section,

and

(*b*) the data controller has complied with any information notice served on him or her in relation to the matter, and

(*c*) (i) the period of 90 days from the date of the receipt of the application or request referred to in subsection (3) of this section (or that period as extended under subsections (4) and (5) of this section or either of them) has elapsed without the receipt by the data controller of a notice under the said subsection (3), or

(ii) the data controller has received a notice under the said subsection (3) stating that the particular processing proposed to be carried on is likely to comply with the provisions of this Act, or

(iii) the data controller—

(I) has received a notice under the said subsection (3) stating that, if the requirements specified by the Commissioner (which he or she is hereby authorised to specify) and appended to the notice are complied with by the data controller, the processing proposed to be carried on is likely to comply with the provisions of this Act, and

(II) has complied with those requirements.

(7) A person who contravenes subsection (6) of this section shall be guilty of an offence.

(8) An appeal against a notice under subsection (3) of this section or a requirement appended to the notice may be made to and heard and determined by the Court under section 26 of this Act and that section shall apply as if such a notice and such a requirement were specified in subsection (1) of the said section 26.

(9) The Minister, after consultation with the Commissioner, may by regulations amend subsections (3), (4) and (6) of this section by substituting for the number of days for the time being specified therein a different number specified in the regulations.

(10) A data controller shall pay to the Commissioner such fee (if any) as may be prescribed in respect of the consideration by the Commissioner, in relation to proposed processing by the data controller, of the matters referred to in paragraphs (i) and

(ii) of subsection (2) of this section and different fees may be prescribed in relation to different categories of processing.

(11) In this section a reference to a data controller includes a reference to a data processor.]

Annotations

Amendments:

F31 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 13, S.I. No. 207 of 2003.

Editorial Notes:

E33 Power pursuant to section exercised (8.10.2007) by *Data Protection (Processing of Genetic Data) Regulations 2007* (S.I. No. 687 of 2007).

E34 Power pursuant to subs. (10) exercised (1.10.2007) by *Data Protection (Fees) Regulations 2007* (S.I. No. 658 of 2007).

Codes of practice.

13.—(1) The Commissioner shall encourage trade associations and other bodies representing categories of data controllers to prepare codes of practice to be complied with by those categories in dealing with personal data.

F32[(2) The Commissioner shall—

(*a*) where a code of practice (referred to subsequently in this section as a code) so prepared is submitted to him or her for consideration, consider the code and, after such consultation with such data subjects or persons representing data subjects and with the relevant trade associations or other bodies aforesaid as appears to him or her to be appropriate—

(i) if he or she is of opinion that the code provides for the data subjects concerned a measure of protection with regard to personal data relating to them that conforms with that provided for by section 2, sections 2A to 2D (inserted by the *Act of 2003*) and sections 3 and 4 (other than subsection (8)) and 6 of this Act, approve of the code and encourage its dissemination to the data controllers concerned, and

(ii) in any event notify the association or body concerned of his or her decision to approve or not to approve the code,

(*b*) where he or she considers it necessary or desirable to do so and after such consultation with any trade associations or other bodies referred to in subsection (1) of this section having an interest in the matter and data subjects or persons representing data subjects as he or she considers appropriate, prepare, and arrange for the dissemination to such persons as he or she considers appropriate of, codes of practice for guidance as to good practice in dealing with personal data, and subsection (3) of this section shall apply to a code of practice prepared under this subsection as it applies to a code,

(*c*) in such manner and by such means as he or she considers most effective for the purposes of this paragraph, promote the following of good practice by data controllers and, in particular, so perform his or her functions under this Act as to promote compliance with this Act by data controllers,

(*d*) arrange for the dissemination in such form and manner as he or she considers appropriate of such information as appears to him or her to be expedient to give to the public about the operation of this Act, about the practices in

87

processing of personal data (including compliance with the requirements of this Act) that appear to the Commissioner to be desirable having regard to the interests of data subjects and other persons likely to be affected by such processing and about other matters within the scope of his or her functions under this Act, and may give advice to any person in relation to any of those matters.]

(3) Any such code that is so approved of may be laid by the Minister before each House of the Oireachtas and, if each such House passes a resolution approving of it, then—

(*a*) in so far as it relates to dealing with personal data by the categories of data controllers concerned—

(i) it shall have the force of law in accordance with its terms, and

(ii) upon its commencement, references (whether specific or general) in this Act to any of the provisions of the said sections shall be construed (or, if the code is in substitution for a code having the force of law by virtue of this subsection, continue to be construed) as if they were also references to the relevant provisions of the code for the time being having the force of law,

and

(*b*) it shall be deemed to be a statutory instrument to which the Statutory Instruments Act, 1947, primarily applies.

(4) This section shall apply in relation to data processors as it applies in relation to categories of data controllers with the modification that the references in this section to the said sections shall be construed as references to *section 2 (1) (d)* of this Act and with any other necessary modifications.

F33[(5) The Commissioner shall be paid by a person in relation to whom a service is provided under this section such fee (if any) as may be prescribed and different fees may be prescribed in relation to different such services and different classes of persons.

(6) In proceedings in any court or other tribunal, any provision of a code, or a code of practice, approved under subsection (3) of this section that appears to the court or other tribunal concerned to be relevant to the proceedings may be taken into account in determining the question concerned.]

Annotations

Amendments:

F32 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 14(1)(a), S.I. No. 207 of 2003.

F33 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 14(1)(b), S.I. No. 207 of 2003.

Modifications (not altering text):

C47 Application of section extended (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 28.

Power to include requirements under these Regulations in codes of practice under the Act of 1988

28. The Commissioner's functions under section 13 of the Act of 1988 extend to requirements imposed under these Regulations.

88

Editorial Notes:

E35 *Data Protection (Amendment) Act 2003* (6/2003), s. 14(2) provides for the continuation in force of a code of practice approved under s. 13(2) before its amendment. It appears that no such code of practice exists.

E36 Previous affecting provision: power of Commissioner extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 17L as inserted (20.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35, subject to transitional provisions in reg. 34.

Annual report.

14.—(1) The Commissioner shall in each year after the year in which the first Commissioner is appointed prepare a report in relation to his F34[activities under the European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003 and this Act] in the preceding year and cause copies of the report to be laid before each House of the Oireachtas.

(2) Notwithstanding *subsection (1)* of this section, if, but for this subsection, the first report under that subsection would relate to a period of less than 6 months, the report shall relate to that period and to the year immediately following that period and shall be prepared as soon as may be after the end of that year.

F35[(3) For the purposes of the law of defamation, a report under subsection (1) shall be absolutely privileged.]

Annotations

Amendments:

F34 Substituted (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 23(1) as amended (20.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 10 which provides that '[t]he reference in Regulation 23(1) of the Principal Regulations to the Data Protection Acts 1988 and 2003 is to be read as, and is to be always taken to have been, a reference to the Data Protection Act 1988 (as amended by the Data Protection Act 2003)'.

F35 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 15, S.I. No. 207 of 2003.

Editorial Notes:

E37 The *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* mentioned in subs. (1) were repealed and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011*, S.I. No. 336 of 2011, reg. 35, subject to transitional provisions in reg. 34.

E38 Previous affecting provision: subs. (1) amended (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 19; amendment substituted as per F-note above.

Mutual assistance between parties to Convention.

15.—(1) The Commissioner is hereby designated for the purposes of Chapter IV (which relates to mutual assistance) of the Convention.

89

(2) The Minister may make any regulations that he considers necessary or expedient for the purpose of enabling the said Chapter IV to have full effect.

Registration

The register.

16.—F36[(1) In this section 'person to whom this section applies' means a data controller and a data processor (other than such (if any) categories of data controller and data processor as may be specified in regulations made by the Minister after consultation with the Commissioner) except in so far as—

(*a*) they carry out—

(i) processing whose sole purpose is the keeping in accordance with law of a register that is intended to provide information to the public and is open to consultation either by the public in general or by any person demonstrating a legitimate interest,

(ii) processing of manual data (other than such categories, if any, of such data as may be prescribed), or

(iii) any combination of the foregoing categories of processing,

or

(*b*) the data controller is a body that is not established or conducted for profit and is carrying out processing for the purposes of establishing or maintaining membership of or support for the body or providing or administering activities for individuals who are either members of the body or have regular contact with it.]

(2) The Commissioner shall establish and maintain a register (referred to in this Act as the register) of persons to whom this section applies and shall make, as appropriate, an entry or entries in the register in respect of each person whose application for registration therein is accepted by the Commissioner.

(3) (*a*) Members of the public may inspect the register free of charge at all reasonable times and may take copies of, or of extracts from, entries in the register.

(*b*) A member of the public may, on payment to the Commissioner of such fee (if any) as may be prescribed, obtain from the Commissioner a copy (certified by him or by a member of his staff to be a true copy) of, or of an extract from, any entry in the register.

(*c*) In any proceedings—

(i) a copy of, or of an extract from, an entry in the register certified by the Commissioner or by a member of his staff to be a true copy shall be evidence of the entry or extract, and

(ii) a document purporting to be such a copy, and to be certified, as aforesaid shall be deemed to be such a copy and to be so certified unless the contrary is proved.

(*d*) In any proceedings—

(i) a certificate signed by the Commissioner or by a member of his staff and stating that there is not an entry in the register in respect of a specified person as a data controller or as a data processor shall be evidence of that fact, and

(ii) a document purporting to be such a certificate, and to be signed, as aforesaid shall be deemed to be such a certificate and to be so signed unless the contrary is proved.

90

Annotations

Amendments:

F36 Substituted (1.10.2007) by *Data Protection (Amendment) Act 2003* (6/2003), s. 16, S.I. No. 656 of 2007.

Editorial Notes:

E39 Power pursuant to subs. (1) exercised (1.10.2007) by *Data Protection Act 1988 (Section 16(1)) Regulations 2007* (S.I. No. 657 of 2007).

E40 Power pursuant to section exercised (16.12.1988) by *Data Protection (Fees) Regulations 1988* (S.I. No. 347 of 1988); regs. 5 and 6 revoked (4.04.1990) by *Data Protection (Fees) Regulations 1990* (S.I. No. 80 of 1990), reg. 5.

E41 Previous affecting provision: power pursuant to subs. (1)(e) exercised (10.1.2001) by *Data Protection (Registration) Regulations 2001* (S.I. No. 2 of 2001); revoked (1.10.2007) by *Data Protection Act 1988 (Section 16(1)) Regulations 2007* (S.I. No. 657 of 2007), reg. 5.

Applications for registration.

17.—(1) (*a*) A person wishing to be registered in the register or to have a registration continued under *section 18* of this Act or to have the particulars in an entry in the register altered shall make an application in writing in that behalf to the Commissioner and shall furnish to him such information as may be prescribed and any other information that he may require.

F37[(*b*) Where a data controller intends to keep personal data for two or more related purposes, he or she shall make an application for registration in respect of those purposes and, subject to the provisions of this Act, entries shall be made in the register in accordance with any such application,]

F38[(*c*) Where a data controller intends to keep personal data for two or more unrelated purposes, he shall make an application for separate registration in respect of each of those purposes and, subject to the provisions of this Act, entries shall be made in the register in accordance with each such application.]

(2) Subject to *subsection (3)* of this section, the Commissioner shall accept an application for registration, made in the prescribed manner and in respect of which such fee as may be prescribed has been paid, from a person to whom *section 16* of this Act applies unless he is of opinion that—

(*a*) the particulars proposed for inclusion in an entry in the register are insufficient or any other information required by the Commissioner either has not been furnished or is insufficient, or

(*b*) the person applying for registration is likely to contravene any of the provisions of this Act.

F37[(3) The Commissioner shall not accept such an application for registration as aforesaid from a data controller who keeps sensitive personal data unless he or she is of opinion that appropriate safeguards for the protection of the privacy of the data subjects are being, and will continue to be, provided by him or her.]

(4) Where the Commissioner refuses an application for registration, he shall, as soon as may be, notify in writing the person applying for registration of the refusal and the notification shall—

(*a*) specify the reasons for the refusal, and

91

(*b*) state that the person may appeal to the Court under *section 26* of this Act against the refusal within 21 days from the receipt by him of the notification.

(5) If—

(*a*) the Commissioner, by reason of special circumstances, is of opinion that a refusal of an application for registration should take effect urgently, and

(*b*) the notification of the refusal includes a statement to that effect and a statement of the effect of the provisions of *section 26* (other than *subsection (3)*) of this Act,

paragraph (b) of *subsection (4)* of this section shall not apply in relation to the notification and *paragraph (b)* of *subsection (6)* of this section shall be construed and have effect as if for the words from and including "21 days" to the end of the paragraph there were substituted "7 days beginning on the date on which the notification was received,".

(6) Subject to *subsection (5)* of this section, a person who has made an application for registration shall—

(*a*) until he is notified that it has been accepted or it is withdrawn, or

(*b*) if he is notified that the application has been refused, until the end of the period of 21 days within which an appeal may be brought under *section 26* of this Act against the refusal and, if such an appeal is brought, until the determination or withdrawal of the appeal,

be treated for the purposes of *section 19* of this Act as if the application had been accepted and the particulars contained in it had been included in an entry in the register on the date on which the application was made.

(7) *Subsections (2)* to *(6)* of this section apply, with any necessary modifications, to an application for continuance of registration and an application for alteration of the particulars in an entry in the register as they apply to an application for registration.

Annotations

Amendments:

F37 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 17(a)(i) and (b), S.I. No. 207 of 2003.

F38 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 17(a)(ii), S.I. No. 207 of 2003.

Editorial Notes:

E42 Power pursuant to section exercised (1.10.2007) by *Data Protection (Fees) Regulations 2007* (S.I. No. 658 of 2007).

E43 Power pursuant to section exercised (16.12.1988) by *Data Protection (Fees) Regulations 1988* (S.I. No. 347 of 1988); regs. 5 and 6 revoked (4.04.1990) by *Data Protection (Fees) Regulations 1990* (S.I. No. 80 of 1990), reg. 5.

E44 Previous affecting provision: power pursuant to section exercised (19.05.1996) by *Data Protection (Fees) Regulations 1996* (S.I. No. 105 of 1996); revoked (1.10.2007) by *Data Protection (Fees) Regulations 2007* (S.I. 658 of 2007), reg. 6.

E45 Previous affecting provision: power pursuant to section exercised (4.04.1990) by *Data Protection (Fees) Regulations 1990* (S.I. No. 80 of 1990); revoked (19.05.1996) by *Data Protection (Fees) Regulations 1996* (S.I. No. 105 of 1996), reg. 5.

92

Duration and continuance of registration.

18.—(1) A registration (whether it is the first registration or a registration continued under this section) shall be for the prescribed period and on the expiry thereof the relevant entry shall be removed from the register unless the registration is continued as aforesaid.

F39[(2) The prescribed period (which shall not be less than one year) shall be calculated—

(*a*) in the case of a first registration from the date on which the relevant entry was made in the register, and

(*b*) in the case of a registration which has been continued under this section, from the day following the expiration of the latest prescribed period.]

(3) The Commissioner shall, subject to the provisions of this Act, continue a registration, whether it has previously been continued under this section or not.

(4) Notwithstanding the foregoing provisions of this section, the Commissioner may at any time, at the request of the person to whom an entry relates, remove it from the register.

Annotations

Amendments:

F39 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 18, S.I. No. 207 of 2003.

Editorial Notes:

E46 Power pursuant to section exercised (15.12.1988) by *Data Protection (Registration Period) Regulations 1988* (S.I. No. 350 of 1988).

Effect of registration.

19.—(1) A data controller to whom *section 16* of this Act applies shall not keep personal data unless there is for the time being an entry in the register in respect of him.

(2) A data controller in respect of whom there is an entry in the register shall not—

(*a*) keep personal data of any description other than that specified in the entry,

(*b*) keep or use personal data for a purpose other than the purpose or purposes described in the entry,

(*c*) if the source from which such data, and any information intended for inclusion in such data, are obtained is required to be described in the entry, obtain such data or information from a source that is not so described,

(*d*) disclose such data to a person who is not described in the entry (other than a person to whom a disclosure of such data may be made in the circumstances specified in *section 8* of this Act),

(*e*) directly or indirectly transfer such data to a place outside the State other than one named or described in the entry.

(3) An employee or agent (not being a data processor) of a data controller mentioned in *subsection (2)* of this section shall, as respects personal data kept or, as the case may be, to be kept by the data controller, be subject to the same restrictions in relation to the use, source, disclosure or transfer of the data as those to which the data controller is subject under that subsection.

93

(4) A data processor to whom *section 16* applies shall not process personal data unless there is for the time being an entry in the register in respect of him.

(5) If and whenever a person in respect of whom there is an entry in the register changes his address, he shall thereupon notify the Commissioner of the change.

(6) A person who contravenes *subsection (1), (4)* or *(5)*, or knowingly contravenes any other provision, of this section shall be guilty of an offence.

Regulations for registration.

20.—(1) The following matters, and such other matters (if any) as may be necessary or expedient for the purpose of enabling *sections 16* to *19* of this Act to have full effect, may be prescribed:

(*a*) the procedure to be followed in relation to applications by persons for registration, continuance of registration or alteration of the particulars in an entry in the register or for withdrawal of such applications,

(*b*) the information required to be furnished to the Commissioner by such persons, and

(*c*) the particulars to be included in entries in the register,

and different provision may be made in relation to the matters aforesaid as respects different categories of persons.

(2) A person who in purported compliance with a requirement prescribed under this section furnishes information to the Commissioner that the person knows to be false or misleading in a material respect shall be guilty of an offence.

Annotations

Editorial Notes:

E47 Power pursuant to section exercised (9.01.1989) by *Data Protection (Registration) Regulations 1988* (S.I. No. 351 of 1988).

Miscellaneous

Unauthorised disclosure by data processor.

21.—(1) Personal data processed by a data processor shall not be disclosed by him, or by an employee or agent of his, without the prior authority of the data controller on behalf of whom the data are processed.

(2) A person who knowingly contravenes *subsection (1)* of this section shall be guilty of an offence.

Disclosure of personal data obtained without authority.

22.—(1) A person who—

(*a*) obtains access to personal data, or obtains any information constituting such data, without the prior authority of the data controller or data processor by whom the data are kept, and

(*b*) discloses the data or information to another person,

shall be guilty of an offence.

(2) *Subsection (1)* of this section does not apply to a person who is an employee or agent of the data controller or data processor concerned.

94

F40[Journalism, literature and art.

22A.—(1) Personal data that are processed only for journalistic, artistic or literary purposes shall be exempt from compliance with any provision of this Act specified in subsection (2) of this section if—

(*a*) the processing is undertaken solely with a view to the publication of any journalistic, literary or artistic material,

(*b*) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, such publication would be in the public interest, and

(*c*) the data controller reasonably believes that, in all the circumstances, compliance with that provision would be incompatible with journalistic, artistic or literary purposes.

(2) The provisions referred to in subsection (1) of this section are—

(*a*) section 2 (as amended by the Act of 2003), other than subsection (1)(*d*),

(*b*) sections 2A, 2B and 2D (which sections were inserted by the Act of 2003),

(*c*) section 3,

(*d*) sections 4 and 6 (which sections were amended by the Act of 2003), and

(*e*) sections 6A and 6B (which sections were inserted by the Act of 2003).

(3) In considering for the purposes of subsection (1)(*b*) of this section whether publication of the material concerned would be in the public interest, regard may be had to any code of practice approved under subsections (1) or (2) of section 13 (as amended by the Act of 2003) of this Act.

(4) In this section 'publication', in relation to journalistic, artistic or literary material, means the act of making the material available to the public or any section of the public in any form or by any means.]

Annotations

Amendments:

F40 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 21, S.I. No. 207 of 2003.

Editorial Notes:

E48 The side-note is taken from the amending section in the absence of one included in the amendment.

Provisions in relation to certain non-residents and to data kept or processed outside State.

23.—F41[...]

95

Annotations

Amendments:

F41 Repealed (1.04.2002) by *European Communities (Data Protection) Regulations 2001* (S.I. No. 626 of 2001), reg. 6 and (1.10.2007) by *Data Protection (Amendment) Act 2003* (6/2003), s. 22(1), S.I. No. 656 of 2007.

Powers of authorised officers.

24.—(1) In this section "authorised officer" means a person authorised in writing by the Commissioner to exercise, for the purposes of this Act, the powers conferred by this section.

(2) An authorised officer may, for the purpose of obtaining any information that is necessary or expedient for the performance by the Commissioner of his functions, on production of the officer's authorisation, if so required—

(*a*) at all reasonable times enter premises that he reasonably believes to be occupied by a data controller or a data processor, inspect the premises and any data therein (other than data consisting of information specified in *section 12 (4) (b)* of this Act) and inspect, examine, operate and test any data equipment therein,

(*b*) require any person on the premises, being a data controller, a data processor or an employee of either of them, to disclose to the officer any such data and produce to him any data material (other than data material consisting of information so specified) that is in that person's power or control and to give to him such information as he may reasonably require in regard to such data and material,

(*c*) either on the premises or elsewhere, inspect and copy or extract information from such data, or inspect and copy or take extracts from such material, and

(*d*) require any person mentioned in *paragraph (b)* of this subsection to give to the officer such information as he may reasonably require in regard to the procedures employed for complying with the provisions of this Act, the sources from which such data are obtained, the purposes for which they are kept, the persons to whom they are disclosed and the data equipment in the premises.

(3) F42[...]

(4) F42[...]

(5) F42[...]

(6) A person who obstructs or impedes an authorised officer in the exercise of a power, or, without reasonable excuse, does not comply with a requirement, under this section or who in purported compliance with such a requirement gives information to an authorised officer that he knows to be false or misleading in a material respect shall be guilty of an offence.

Annotations

Amendments:

F42 Repealed (1.10.2007) by *Data Protection (Amendment) Act 2003* (6/2003), s. 22(1), S.I. No. 656 of 2007.

96

Modifications (not altering text):

C48 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C49 Application of section extended with any necessary modifications (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

Unsolicited commercial communications.

9. ...

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

...

(10) Section 24 of the Act applies as if —

(a) in subsection (2)(a), there were substituted "a person to whom the Regulations of 2003 apply" for "a data controller or a data processor",

(b) in subsection (2)(b), there were substituted "being a person to whom the Regulations of 2003 apply or an employee of such a person" for "being a data controller, a data processor or an employee of either of them",

(c) there were deleted subsections (3), (4) and (5).

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

Editorial Notes:

E49 Previous affecting provision: section applied with modifications (from the date on which the declaration by the State under Article 32(4) of the Customs Co-operation Convention took effect to 24 October 2007) by *Customs and Excise (Mutual Assistance) Act 2001 (Section 8) (Protection of Manual Data) Regulations 2004* (S.I. No. 254 of 2004), reg. 10(2).

97

E50 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35 subject to transitional provisions in reg. 34.

E51 Previous affecting provision: application of ss. 10, 12, 24, 25, 26 (insofar as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Commissioner in relation to a complaint under section 10(1)(a)) and ss. 27 to 31 extended with any necessary modifications (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 12; revoked (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 24.

Service of notices.

25.—Any notice authorised by this Act to be served on a person by the Commissioner may be served—

(*a*) if the person is an individual—

(i) by delivering it to him or

(ii) by sending it to him by post addressed to him at his usual or last-known place of residence or business, or

(iii) by leaving it for him at that place,

(*b*) if the person is a body corporate or an unincorporated body of persons, by sending it to the body by post to, or addressing it to and leaving it at, in the case of a company, its registered office (within the meaning of the Companies Act, 1963) and, in any other case, its principal place of business.

Annotations

Modifications (not altering text):

C50 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C51 Application of section extended with any necessary modifications (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

Unsolicited commercial communications.

98

9. ...

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

...

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

...

Editorial Notes:

E52 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35 subject to transitional provisions in reg. 34.

E53 Previous affecting provision: application of ss. 10, 12, 24, 25, 26 (insofar as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Commissioner in relation to a complaint under section 10(1)(a)) and ss. 27 to 31 extended with any necessary modifications (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 12; revoked (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 24.

Appeals to Circuit Court.

26.—(1) An appeal may be made to and heard and determined by the Court against—

(*a*) a requirement specified in an enforcement notice or an information notice,

(*b*) a prohibition specified in a prohibition notice,

(*c*) a refusal by the Commissioner under *section 17* of this Act, notified by him under that section, and

(*d*) a decision of the Commissioner in relation to a complaint under *section 10 (1) (a)* of this Act,

and such an appeal shall be brought within 21 days from the service on the person concerned of the relevant notice or, as the case may be, the receipt by such person of the notification of the relevant refusal or decision.

(2) The jurisdiction conferred on the Court by this Act shall be exercised by the judge for the time being assigned to the circuit where the appellant ordinarily resides

99

or carries on any profession, business or occupation or, at the option of the appellant, by a judge of the Court for the time being assigned to the Dublin circuit.

(3) (*a*) Subject to *paragraph (b)* of this subsection, a decision of the Court under this section shall be final.

(*b*) An appeal may be brought to the High Court on a point of law against such a decision; and references in this Act to the determination of an appeal shall be construed as including references to the determination of any such appeal to the High Court and of any appeal from the decision of that Court.

(4) Where—

(*a*) a person appeals to the Court pursuant to *paragraph (a), (b)* or *(c)* of *subsection (1)* of this section,

(*b*) the appeal is brought within the period specified in the notice or notification mentioned in *paragraph (c)* of this subsection, and

(*c*) the Commissioner has included a statement in the relevant notice or notification to the effect that by reason of special circumstances he is of opinion that the requirement or prohibition specified in the notice should be complied with, or the refusal specified in the notification should take effect, urgently,

then, notwithstanding any provision of this Act, if the Court, on application to it in that behalf, so determines, non-compliance by the person with a requirement or prohibition specified in the notice, or, as the case may be, a contravention by him of *section 19* of this Act, during the period ending with the determination or withdrawal of the appeal or during such other period as may be determined as aforesaid shall not constitute an offence.

Annotations

C52 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

Editorial Notes:

E54 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9.

100

Evidence in proceedings.

27.—(1) In any proceedings—

(*a*) a certificate signed by the Minister or the Minister for Defence and stating that in his opinion personal data are, or at any time were, kept for the purpose of safeguarding the security of the State shall be evidence of that opinion,

(*b*) a certificate—

(i) signed by a member of the Garda Síochána not below the rank of chief superintendent or an officer of the Permanent Defence Force who holds an army rank not below that of colonel and is designated by the Minister for Defence under *section 8 (a)* of this Act, and

(ii) stating that in the opinion of the member or, as the case may be, the officer a disclosure of personal data is required for the purpose aforesaid,

shall be evidence of that opinion, and

(*c*) a document purporting to be a certificate under *paragraph (a)* or *(b)* of this subsection and to be signed by a person specified in the said *paragraph (a)* or *(b)*, as appropriate, shall be deemed to be such a certificate and to be so signed unless the contrary is proved.

(2) Information supplied by a person in compliance with a request under *section 3* or *4 (1)* of this Act, a requirement under this Act or a direction of a court in proceedings under this Act shall not be admissible in evidence against him or his spouse in proceedings for an offence under this Act.

Annotations

Modifications (not altering text):

C53 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C54 Application of section extended with any necessary modifications (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

Unsolicited commercial communications.

9. ...

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

101

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

...

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

...

Editorial Notes:

E55 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9.

E56 Previous affecting provision: application of ss. 10, 12, 24, 25, 26 (insofar as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Commissioner in relation to a complaint under section 10(1)(a)) and ss. 27 to 31 extended with any necessary modifications (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 12; revoked (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 24.

Hearing of proceedings.

28.—The whole or any part of any proceedings under this Act may, at the discretion of the court, be heard otherwise than in public.

Annotations

Modifications (not altering text):

C55 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C56 Application of section extended with any necessary modifications (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

102

Unsolicited commercial communications.

9. ...

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

...

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

...

Editorial Notes:

E57 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35 subject to transitional provisions in reg. 34.

E58 Previous affecting provision: application of ss. 10, 12, 24, 25, 26 (insofar as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Commissioner in relation to a complaint under section 10(1)(a)) and ss. 27 to 31 extended with any necessary modifications (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 12; revoked (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 24.

Offences by directors, etc., of bodies corporate.

29.—(1) Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of a person, being a director, manager, secretary or other officer of that body corporate, or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, *subsection (1)* of this section shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director or manager of the body corporate.

Annotations

Modifications (not altering text):

C58 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C59 Application of section extended with any necessary modifications (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

Unsolicited commercial communications.

9. ...

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

...

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

...

Editorial Notes:

E59 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35 subject to transitional provisions in reg. 34.

E60 Previous affecting provision: application of ss. 10, 12, 24, 25, 26 (insofar as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Commissioner in relation to a complaint under section 10(1)(a)) and ss. 27 to 31 extended with any necessary modifications (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 12; revoked (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 24.

Prosecution of summary offences by Commissioner.

30.—(1) Summary proceedings for an offence under this Act may be brought and prosecuted by the Commissioner.

(2) Notwithstanding section 10 (4) of the Petty Sessions (Ireland) Act, 1851, summary proceedings for an offence under this Act may be instituted within on e year from the date of the offence.

Annotations

Modifications (not altering text):

C61 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C62 Application of section extended with any necessary modifications (24.02.2003) by *European Communities (Directive 2000/31/EC) Regulations 2003* (S.I. No. 68 of 2003), reg. 9(6).

Unsolicited commercial communications.

9. ...

(6) The following provisions of the Act, namely —

(a) sections 1, 10, 12, 24 and 25,

(b) section 26 in so far as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Data Protection Commissioner in relation to a complaint under section 10 (1) (a) of the Act,

and

(c) sections 27 to 30,

apply for the purpose of this Regulation with the modifications specified in paragraphs (7) to (10) and any other necessary modifications.

(7) References, in the provisions of the Act mentioned in paragraph (6), to that Act or the provisions of that Act shall, unless the context otherwise requires be construed as including references to this Regulation or the provisions of this Regulation.

...

105

(11) In this Regulation —

"Act" means the Data Protection Act 1988 (No. 25 of 1988);

...

Editorial Notes:

E61 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35 subject to transitional provisions in reg. 34.

E62 Previous affecting provision: application of ss. 10, 12, 24, 25, 26 (insofar as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Commissioner in relation to a complaint under section 10(1)(a)) and ss. 27 to 31 extended with any necessary modifications (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 12; revoked (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 24.

Penalties.

31.—(1) A person guilty of an offence under this Act shall be liable—

(*a*) on summary conviction, to a fine not exceeding F43[€3,000], or

(*b*) on conviction on indictment, to a fine not exceeding F43[€100,000].

(2) Where a person is convicted of an offence under this Act, the court may order any data material which appears to the court to be connected with the commission of the offence to be forfeited or destroyed and any relevant data to be erased.

(3) The court shall not make an order under *subsection (2)* of this section in relation to data material or data where it considers that some person other than the person convicted of the offence concerned may be the owner of, or otherwise interested in, the data unless such steps as are reasonably practicable have been taken for notifying that person and giving him an opportunity to show cause why the order should not be made.

(4) Section 13 of the Criminal Procedure Act, 1967, shall apply in relation to an offence under this Act that is not being prosecuted summarily as if, in lieu of the penalties provided for in subsection (3) (*a*) of that section, there were specified therein the fine provided for in *subsection (1) (a)* of this section and the reference in subsection (2) (*a*) of the said section 13 to the penalties provided for by subsection (3) shall be construed and have effect accordingly.

Annotations

Amendments:

F43 Substituted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 19, S.I. No. 207 of 2003.

Modifications (not altering text):

C64 Application of section extended with modification (27.01.2014) by *Credit Reporting Act 2013* (45/2013), s. 19(2), (4), S.I. No. 19 of 2014.

Data protection

19. ...

(2) Sections 2 , 4 and 6 of the Data Protection Act 1988 shall have effect as if—

(a) references to personal data included relevant credit data, and

(b) a person to whom this section applies were a living individual, and sections 9, 10, 12 and 24 to 31 of that Act apply accordingly.

(3) ...

(4) This section applies to any person with an annual turnover of not more than €3,000,000 (and to whom sections 2, 4 and 6 of the Data Protection Act 1988 would not apply apart from this section).

...

C65 Application of Act extended (31.12.2005) by *Disability Act 2005* (14/2005), s. 42(4), S.I. No. 474 of 2005.

Genetic testing and processing of genetic data.

42.—...

(4) A person who contravenes *subsection (2)* or *(3)* shall be guilty of an offence; an offence under this subsection shall be deemed to be an offence to which section 31 of the Data Protection Act 1988 applies.

Editorial Notes:

E63 Previous affecting provision: construction of section extended (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2008* (S.I. No. 535 of 2003), reg. 17(1)(a); reg. 17 substituted (13.12.2008) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008* (S.I. No. 526 of 2008), reg. 9; revoked and replaced (1.07.2011) by *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (S.I. No. 336 of 2011), reg. 35 subject to transitional provisions in reg. 34.

E64 Previous affecting provision: application of ss. 10, 12, 24, 25, 26 (insofar as it relates to a requirement specified in an enforcement notice or an information notice or a decision of the Commissioner in relation to a complaint under section 10(1)(a)) and ss. 27 to 31 extended with any necessary modifications (8.05.2002) by *European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002* (S.I. No. 192 of 2002), reg. 12; revoked (6.11.2003) by *European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003* (S.I. No. 535 of 2003), reg. 24.

Laying of regulations before Houses of Oireachtas.

32.—Every regulation made under this Act (other than *section 2*) shall be laid before each House of the Oireachtas as soon as may be after it is made and, if a resolution annulling the regulation is passed by either such House within the next 21 days on which that House has sat after the regulation is laid before it, the regulation shall be annulled accordingly, but without prejudice to the validity of anything previously done thereunder.

Fees.

33.—(1) Fees under this Act shall be paid into or disposed of for the benefit of the Exchequer in accordance with the directions of the Minister for Finance.

(2) The Public Offices Fees Act, 1879, shall not apply in respect of any fees under this Act.

107

Annotations

Modifications (not altering text):

C66 Functions transferred and references to "Department of Finance" and "Minister for Finance" construed (29.07.2011) by *Finance (Transfer of Departmental Administration and Ministerial Functions) Order 2011* (S.I. No. 418 of 2011), arts. 2, 3, 5 and sch. 1 part 2, in effect as per art. 1(2), subject to transitional provisions in arts. 6-9.

2. (1) The administration and business in connection with the performance of any functions transferred by this Order are transferred to the Department of Public Expenditure and Reform.

(2) References to the Department of Finance contained in any Act or instrument made thereunder and relating to the administration and business transferred by paragraph (1) shall, on and after the commencement of this Order, be construed as references to the Department of Public Expenditure and Reform.

3. The functions conferred on the Minister for Finance by or under the provisions of —

(a) the enactments specified in Schedule 1, and

(b) the statutory instruments specified in Schedule 2,

are transferred to the Minister for Public Expenditure and Reform.

...

5. References to the Minister for Finance contained in any Act or instrument under an Act and relating to any functions transferred by this Order shall, from the commencement of this Order, be construed as references to the Minister for Public Expenditure and Reform.

...

Schedule 1

Enactments

...

Part 2

1922 to 2011 Enactments

Number and Year	Short Title	Provision
(1)	(2)	(3)
...	...	...
No. 25 of 1988	Data Protection Act 1988	Sections 1 and 33(1); Second Schedule, paragraph 9
...	...	...

Expenses of Minister.

34.—The expenses incurred by the Minister in the administration of this Act shall, to such extent as may be sanctioned by the Minister for Finance, be paid out of moneys provided by the Oireachtas.

Short title and commencement.

35.—(1) This Act may be cited as the Data Protection Act, 1988.

(2) This Act shall come into operation on such day or days as, by order or orders made by the Minister under this section, may be fixed therefor either generally or with reference to any particular purpose or provision and different days may be so fixed for different purposes and different provisions.

108

Annotations

Editorial Notes:

E65 Power pursuant to section exercised (18.07.2014) by *Data Protection Act 1988 (Commencement) Order 2014* (S.I. No. 337 of 2014).

2. The 18th day of July 2014 is fixed as the day on which the Data Protection Act 1988 (No. 25 of 1988), insofar as it is not already in operation, shall come into operation.

E66 Power pursuant to subs. (2) exercised (19.12.1988) by *Data Protection Act (Commencement) Order 1988* (S.I. No. 349 of 1988).

3. The 9th day of January, 1989, is hereby fixed as the day on which the following provisions of the Act shall come into operation, namely:

(*a*) sections 1, 9, 16 (other than subsection (3)), 17, 18, 20,26 (other than paragraphs (*a*), (*b*) and (*d*) of subsection (1) and subsection (4)), 32 to 35, and

(*b*) the Second and Third Schedules.

4. The 19th day of April, 1989, is hereby fixed as the day on which the Act (other than sections 6 (2) (*b*) and 10 (7) (*b*) and the provisions specified in Regulation 3 of these Regulations) shall come into operation.

Section 1 (1).

FIRST SCHEDULE

CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981

PREAMBLE

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

CHAPTER I—GENERAL PROVISIONS

Article 1

Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2

Definitions

For the purposes of this convention:

a. "personal data" means any information relating to an identified or identifiable individual ("data subject");

b. "automated data file" means any set of data undergoing automatic processing;

c. "automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3

Scope

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;

b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c. that it will also apply this convention to personal data files which are not processed automatically.

3. Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.*b* or *c* above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.*a* above may not claim the application of this convention to such categories by a Party which has not excluded them.

5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.*b* or *c* above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

CHAPTER II—BASIC PRINCIPLES FOR DATA PROTECTION

Article 4

Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5

Quality of data

111

Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6

Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7

Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8

Additional safeguards for the data subject

Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9

Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

112

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs *b, c* and *d*, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10

Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11

Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

CHAPTER III—TRANSBORDER DATA FLOWS

Article 12

Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

CHAPTER IV—MUTUAL ASSISTANCE

Article 13

Co-operation between Parties

1. The Parties agree to render each other mutual assistance in order to implement this convention.

2. For that purpose:

a. each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;

b. each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.

3. An authority designated by a Party shall at the request of an authority designated by another Party:

a. furnish information on its law and administrative practice in the field of data protection;

b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14

Assistance to data subjects resident abroad

1. Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

2. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

3. The request for assistance shall contain all the necessary particulars, relating *inter alia* to:

a. the name, address and any other relevant particulars identifying the person making the request;

b. the automated personal data file to which the request pertains, or its controller;

c. the purpose of the request.

Article 15

Safeguards concerning assistance rendered by designated authorities

1. An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

2. Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

3. In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16

114

Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless:

a. the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;

b. the request does not comply with the provisions of this convention;

c. compliance with the request would be incompatible with the sovereignty, security or public policy (*ordre public*) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17

Costs and procedures of assistance

1. Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

2. The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.

3. Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

CHAPTER V—CONSULTATIVE COMMITTEE

Article 18

Composition of the committee

1. A Consultative Committee shall be set up after the entry into force of this convention.

2. Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.

3. The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19

Functions of the committee

The Consultative Committee:

a. may make proposals with a view to facilitating or improving the application of the convention;

b. may make proposals for amendment of this convention in accordance with Article 21;

115

c. shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3;

d. may, at the request of a Party, express an opinion on any question concerning the application of this convention.

Article 20

Procedure

1. The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.

2. A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.

3. After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.

4. Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

CHAPTER VI—AMENDMENTS

Article 21

Amendments

1. Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.

3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

CHAPTER VII—FINAL CLAUSES

Article 22

Entry into force

1. This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2. This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

3. In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

Article 23

Accession by non-member States

1. After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.*d* of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

2. In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 24

Territorial clause

1. Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

2. Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25

Reservations

No reservation may be made in respect of the provisions of this convention.

Article 26

Denunciation

1. Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.

117

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27

Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this convention in accordance with Articles 22, 23 and 24;

d. any other act, notification or communication relating to this convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

Section 9.

SECOND SCHEDULE

The Data Protection Commissioner

1. The Commissioner shall be a body corporate and shall be independent in the performance of his functions.

2. (1) The Commissioner shall be appointed by the Government and, subject to the provisions of this Schedule, shall hold office upon such terms and conditions as the Government may determine.

(2) The Commissioner—

(*a*) may at any time resign his office as Commissioner by letter addressed to the Secretary to the Government and the resignation shall take effect on and from the date of receipt of the letter,

(*b*) may at any time be removed from office by the Government if, in the opinion of the Government, he has become incapable through ill-health of effectively performing his functions or has committed stated misbehaviour, and

(*c*) shall, in any case, vacate the office of Commissioner on reaching the age of 65 years F44[: but where the person is a new entrant (within the meaning of the Public Service Superannuation (Miscellaneous Provisions) Act 2004) appointed on or after 1 April 2004, then the requirement to vacate office on grounds of age shall not apply.].

3. The term of office of a person appointed to be the Commissioner shall be such term not exceeding 5 years as the Government may determine at the time of his

118

appointment and, subject to the provisions of this Schedule, he shall be eligible for re-appointment to the office.

4. (1) Where the Commissioner is—

(*a*) nominated as a member of Seanad Éireann,

(*b*) elected as a member of either House of the Oireachtas, the European Parliament or a local authority, or

(*c*) regarded pursuant to section 15 (inserted by the European Assembly Elections Act, 1984) of the European Assembly Elections Act, 1977, as having been elected to such Parliament to fill a vacancy,

he shall thereupon cease to be the Commissioner.

(2) A person who is for the time being—

(i) entitled under the standing orders of either House of the Oireachtas to sit therein,

(ii) a member of the European Parliament, or

(iii) entitled under the standing orders of a local authority to sit therein,

shall, while he is so entitled or is such a member, be disqualified for holding the office of Commissioner.

5. The Commissioner shall not hold any other office or employment in respect of which emoluments are payable.

6. There shall be paid to the Commissioner, out of moneys provided by the Oireachtas, such remuneration and allowances for expenses as the Minister, with the consent of the Minister for Finance, may from time to time determine.

7. (*a*) The Minister shall, with the consent of the Minister for Finance, make and carry out, in accordance with its terms, a scheme or schemes for the granting of pensions, gratuities or other allowances on retirement or death to or in respect of persons who have held the office of Commissioner.

(*b*) The Minister may, with the consent of the Minister for Finance, at any time make and carry out, in accordance with its terms, a scheme or schemes amending or revoking a scheme under this paragraph.

(*c*) A scheme under this paragraph shall be laid before each House of the Oireachtas as soon as may be after it is made and, if a resolution annulling the scheme is passed by either such House within the next 21 days on which that House has sat after the scheme is laid before it, the scheme shall be annulled accordingly, but without prejudice to the validity of anything previously done thereunder.

8. (1) The Minister may appoint to be members of the staff of the Commissioner such number of persons as may be determined from time to time by the Minister, with the consent of the Minister for Finance.

(2) Members of the staff of the Commissioner shall be civil servants.

(3) The functions of the Commissioner under this Act may be performed during his temporary absence by such member of the staff of the Commissioner as he may designate for that purpose.

(4) The Minister may delegate to the Commissioner the powers exercisable by him under the F45[Public Service Management (Recruitment and Appointments) Act 2004],

and the Civil Service Regulation Acts, 1956 and 1958, as the appropriate authority in relation to members of the staff of the Commissioner and, if he does so, then so long as the delegation remains in force—

(*a*) those powers shall, in lieu of being exercisable by the Minister, be exercisable by the Commissioner, and

(*b*) the Commissioner shall, in lieu of the Minister, be for the purposes of this Act the appropriate authority in relation to members of the staff of the Commissioner.

9. (1) The Commissioner shall keep in such form as may be approved of by the Minister, with the consent of the Minister for Finance, all proper and usual accounts of all moneys received or expended by him and all such special accounts (if any) as the Minister, with the consent of the Minister for Finance, may direct.

(2) Accounts kept in pursuance of this paragraph in respect of each year shall be submitted by the Commissioner in the following year on a date (not later than a date specified by the Minister) to the Comptroller and Auditor General for audit and, as soon as may be after the audit, a copy of those accounts, or of such extracts from those accounts as the Minister may specify, together with the report of the Comptroller and Auditor General on the accounts, shall be presented by the Commissioner to the Minister who shall cause copies of the documents presented to him to be laid before each House of the Oireachtas.

F46[10. (1) A person who holds or held the office of Commissioner or who is or was a member of the staff of the Commissioner shall not disclose to a person other than the Commissioner or such a member any information that is obtained by him or her in his capacity as Commissioner or as such a member that could reasonably be regarded as confidential without the consent of the person to whom it relates.

(2) A person who contravenes subparagraph (1) of this paragraph shall be guilty of an offence.]

Annotations

Amendments:

F44 Inserted (25.03.2004) by *Public Service Superannuation (Miscellaneous Provisions) Act 2004* (7/2004), s. 3 and sch. 2 part 2, commenced on enactment.

F45 Substituted (6.10.2004) by *Public Service Management (Recruitment and Appointments) Act 2004* (33/2004), s. 61(1) and sch. 2 part 1, commenced on enactment.

F46 Inserted (1.07.2003) by *Data Protection (Amendment) Act 2003* (6/2003), s. 20, S.I. No. 207 of 2003.

Editorial Notes:

E67 Power pursuant to s. 9 and sch. para. 7(a) exercised (25.05.1993) by *Data Protection Commissioner Superannuation Scheme 1993* (S.I. No. 141 of 1993).

Section 16 (1) (a).

THIRD SCHEDULE

PUBLIC AUTHORITIES AND OTHER BODIES AND PERSONS

120

F47[...]

Annotations

Amendments:

F47 Repealed (1.10.2007) by *Data Protection (Amendment) Act 2003* (6/2003), s. 22(1), S.I. No. 656 of 2007.

121

3

reached a similar conclusion when the child was slightly younger. However, it has not been of direct relevance to my reasoning as only the order and not the reason for same was available to me.

42. For all of the above reasons I decided to refuse the application.

Solicitors for the applicant: *Legal Aid Board*
Solicitors for the respondent: *Legal Aid Board*

Trevor Redmond
Barrister

In the matter of the Data Protection Acts 1988 and 2003, and in the matter of an appeal purportedly pursuant to section 26 of the Data Protection Acts 1988 and 2003, Peter Nowak v Data Protection Commissioner: High Court 2010 No.230CA (Birmingham J.) March 7, 2012 [2012] IEHC 449 ([2013] 1 I.L.R.M. 207)

Data Protection – Data access – Personal data – Whether examination script "personal data" – Whether complaint "frivolous or vexatious" – Appeal – Whether decision of Data Protection Commissioner that complaint was frivolous or vexatious could be appealed to Circuit Court – Deferential standard of review of decision of statutory body – Data Protection Act 1988, ss.10, 26 – Data Protection (Amendment) Act 2003 (No.6), s.11

Facts Section 10(1) of the Data Protection Act 1988 (as amended by s.11 of the Data Protection (Amendment) Act 2003) provides, inter alia, as follows:

> "(a) The Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.
> (b) Where a complaint is made to the Commissioner under paragraph (a) of this subsection, the Commissioner shall -
> (i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious ...."

The appellant was a student with Chartered Accountants Ireland and sat an examination at which he was unsuccessful. The appellant submitted a personal data access request and sought, in particular, a copy of his examination script, but access to his examination script was refused on the ground that the examination

script did not constitute "personal data" within the meaning of the Data Protection Acts 1988–2003. The appellant was, however, afforded an opportunity to inspect his examination script at a particular time and under controlled conditions, but the appellant never availed of this option.

The appellant made a formal complaint to the Data Protection Commissioner ("the respondent"). On July 21, 2010 the respondent replied to the appellant and informed him that it had been concluded that the appellant had not identified any substantial breach of the Data Protections Acts and in accordance with s.10(1)(b)(i) of the Data Protection Acts the respondent was not obliged to investigate the complaint on the ground it was "frivolous or vexatious".

The appellant appealed to the Circuit Court pursuant to s.26 of the Data Protection Act 1988. The Circuit Court held the court did not have jurisdiction to hear an appeal from a decision of the respondent not to investigate a complaint on the ground it was "frivolous or vexatious". However, if the court did have jurisdiction it would have upheld the view of the respondent that the appellant's examination script did not constitute "personal data". The appellant appealed to the High Court against the judgment and order of the Circuit Court.

Held by Birmingham J. in dismissing the appeal and affirming the order of the Circuit Court:

(1) The Circuit Court's jurisdiction to hear and determine an appeal against a decision of the Data Protection Commissioner to decline to investigate a complaint because he has formed the view that it is frivolous or vexatious depends on whether reaching that conclusion involves a decision which can be the subject of an appeal under s.26 of the Data Protection Acts.

(2) Absent investigation of the complaint and a decision to relation to the investigation by the Data Protection Commissioner, the Circuit Court has no jurisdiction. The Commissioner reaches a decision in relation to a complaint only if, not having decided that the matter is frivolous or vexatious, he proceeds to investigate the complaint and reaches a decision in relation thereto. Once the Commissioner formed the view that the examination script did not constitute personal data it followed that he was being asked to proceed with an investigation where no breach of the Data Protection Acts could be identified. It was in those circumstances that the complaint was "frivolous or vexatious".

(3) The terms "frivolous or vexatious" are not necessarily pejorative. "Frivolous", in this context, means a complaint that was futile, or misconceived or hopeless in the sense that it was incapable of achieving the desired outcome. *R. v North West Suffolk (Mildenhall) Magistrates' Court, ex p.Forest Heath District Council* [1997] EWCA Civ. 1575; unreported, Court of Appeal, May 16, 1997 considered.

(4) If the court had jurisdiction to hear the appeal from a statutory body such as the respondent, it would have been appropriate for the court to have regard to the "deferential standard" of review when deciding whether to substitute its

own view for that of the respondent on the issue of whether an examination script constituted personal data. This does not mean that a court will abdicate its responsibilities and there may be cases where decisions will be set aside, but a decision to set aside will be taken by a court that is conscious of the experience and expertise of the statutory body. *Ulster Bank Investment Funds Ltd v Financial Services Ombudsman* [2006] IEHC 323; unreported, High Court, Finnegan P., November 1, 2006 and *Orange Communications v Director of Telecommunications Regulation* [2000] IESC 22; unreported, Supreme Court, May 18, 2000 considered.

(5) The amount of personal information contained in an examination script may vary significantly depending on the nature of the examination, for example, a psychometric test or IQ test would likely contain more information relating to the person that undertook the test than a test of general knowledge. The Commissioner was correct to conclude that the examination script in this case was not "personal data".

Cases referred to in judgment

Orange Communications v Director of Telecommunications Regulation [2000] IESC 22; unreported, Supreme Court, May 18, 2000

R. v North West Suffolk (Mildenhall) Magistrates' Court, ex p.Forest Heath District Council [1997] EWCA Civ. 1575; unreported, Court of Appeal, May 16, 1997

State (Keegan) v Stardust Victims' Compensation Tribunal [1986] I.R. 642; [1987] I.L.R.M. 202 HC, SC

Ulster Bank Investment Funds Ltd v Financial Services Ombudsman [2006] IEHC 323; unreported, High Court, Finnegan P., November 1, 2006.

Proinsias Ó Maolchalain **for the appellant**

Paul Anthony McDermott **for the respondent**

BIRMINGHAM J. delivered his judgment on March 7, 2012 saying:

1. This matter comes before the court by way of an appeal from the judgment of Judge Linnane of November 16, 2010. The background to the matter may be stated briefly. The appellant has registered as a student with Chartered Accountants Ireland (hereinafter "CAI") with a view to gaining a professional qualification as a chartered accountant. He sat an examination on October 7, 2009 but was unsuccessful. By letter dated May 12, 2010, Mr Nowak submitted a personal data access request in which he asked CAI to release to him all personal data within the meaning of that term as set out in the Data Protection Acts 1988 to 2003 (hereinafter "the Data Protection Acts"). The letter specified that in particular he was seeking a copy of his examination script, all personal data relating to his appeal to the appeals panel with regard to his failure in that examination to include any personal data in existence concerning that appeal, any data compiled by the external examiner and appeals panel and any data sent or received by CAI whether in manual or electronic format.

2. A very considerable volume of material was furnished to Mr Nowak by CAI but in correspondence it was made clear to him that the material that would be provided to him would not include his examination script because CAI had received legal advice that the Data Protection Acts did not extend to that material. In passing, it may be noted and it is certainly a very strange feature of this case that although the procedures in relation to examinations conducted by the CAI provided exam candidates with an opportunity to read their scripts at a particular time and under controlled conditions, that Mr Nowak never availed of this option. By letters dated July 1, 2010 and July 14, 2010, Mr Nowak submitted a formal complaint to the Data Protection Commissioner, the respondent. CAI, it may be noted is registered as a "data controller" with the respondent. These written complaints supplemented an earlier online complaint that had been submitted by him on June 17, 2010. While Mr Nowak in the form he completed and in correspondence had raised a number of issues, his principal concern, and this is the only matter that arises on the appeal hearing, was the refusal of CAI to provide him with a copy of his examination script based on the view that it had formed that the script did not constitute "personal data" within the meaning of the Acts. On July 21, 2010, the respondent wrote to the appellant and informed him that having examined all the papers in the matter it had been concluded that Mr Nowak had not identified any substantive breach of the Data Protection Acts. The letter stated:

> "In accordance with s. 10(1)(b)(i) of the Data Protection Acts we are not obliged to investigate a complaint where no substantive breach of the Act remains to be investigated".

3. By a notice of motion dated August 11, 2010 an appeal was brought to the Circuit Court. By letter of even date, the respondent wrote to the appellant's solicitors stating as follows:

> "It is noted that you intend to make an appeal to the Circuit Court under the provisions of the Data Protection Acts 1988 and 2003. You should be aware that the Data Protection Commissioner has not made an appealable decision under the provisions of s.10(1)(b)(ii) of the Data Protection Acts 1988 and 2003. The Commissioner chose not to investigate your client's complaints as he had formed the opinion, in accordance with s.10(1)(b)(i) of the Acts, that they were frivolous or vexatious. The Data Protection Acts do not provide for a right of appeal in such circumstances".

4. The matter came on for hearing before Judge Linnane on November 16, 2010. She determined that the court did not have jurisdiction pursuant to s.26 of the Data Protection Acts to hear an appeal as the Data Commissioner pursuant to s.10(1)(b) of the Acts had declined to investigate the appellant's complaint having formed the view that the complaint was "frivolous or vexatious". She went on

to hold that if she had jurisdiction to hear the appeal that she would have upheld the decision arrived at by the Commissioner and would have agreed with his views that the examination script did not constitute personal data.

5. Section 26(3)(b) of the Data Protection Acts provides that an appeal may be brought to the High Court on a point of law against a decision of the Circuit Court in relation to an appeal that had been brought to it. The notice of appeal in the present case which is dated November 26, 2010 does not specify on what point of law the appeal is brought to the High Court but instead simply states that Mr Nowak appeals the whole of the order of the Circuit Court declaring that the Circuit Court did not have jurisdiction to hear the appeal pursuant to s.26 of the Data Protection Acts and dismissing the appeal and granting the respondent, the Data Protection Commissioner, the costs of the proceedings. However, written submissions have been exchanged and by reference to those and more particularly by reference to the submissions delivered on behalf of the appellant it emerges that the following points of law are said to arise on the hearing of the appeal to this court.

(1) Was the Circuit Court correct to conclude that it had no jurisdiction to hear an appeal in circumstances where the Data Commissioner had not embarked upon an investigation of the merits of the complaint but had declined to do so having formed the view that the complaint was frivolous and vexatious;
(2) If the Circuit Court had jurisdiction should it have determined that the Data Commissioner was correct in concluding that the examination scripts did not constitute "personal data" and;
(3) Should the Circuit Court have concluded that the complaint advanced by Mr Nowak to the Data Commissioner was one that was frivolous and vexatious.

6. Section 10(1) of the Data Protection Acts provides as follows:

"(a) The Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.
(b) Where a complaint is made to the Commissioner under paragraph (a) of this subsection, the Commissioner shall-
(i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious, and
(ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it to the court under section

26 of this Act within 21 days from the receipt by him or her of the notification."

7. Section 26(1) of the Acts so far as material provides that:

"An appeal may be made to and heard and determined by the court against-

...

(d) a decision of the Commissioner in relation to a complaint under section 10(1)(a) of this Act".

Thus, the Circuit Court's jurisdiction is to hear and determine an appeal against a decision of the Commissioner in relation to a complaint under s.10(1)(a) of these Acts. The question then is whether when the Commissioner declines to investigate a complaint because he has formed the view that the subject matter of the complaint is frivolous or vexatious, that reaching that conclusion involves a decision which can be the subject of an appeal.

8. Section 10(1) seems to envisage that the following sequence of events will occur:

(1) The Commissioner has to decide whether the matter submitted to him is frivolous or vexatious.

(2) If the Commissioner is of the view that the matter was not frivolous or vexatious, then, unless an amicable resolution can be arranged within a reasonable time, he considers the matter and reaches a decision in relation to it and then informs the complainant of the decision that has been reached and that the decision may be appealed.

(3) However, if the view is formed that the matter that has been submitted is frivolous or vexatious, then the Commissioner does not investigate the complaint or cause it to be investigated. In that event the procedure comes to a halt.

9. I find myself in respectful agreement with Judge Linnane that the jurisdiction of the Circuit Court is to hear an appeal against a decision that has been arrived at after there has been an investigation. I share her view that absent investigation of the complaint and a decision in relation to the investigation, the Circuit Court has no jurisdiction. The entitlement of an aggrieved party in the first place to submit an appeal and then of the court to hear and determine an appeal arises only where there has been a decision of the Commissioner in relation to a complaint under s.10(1)(a). However, the Commissioner reaches a decision in relation to a complaint only if, not having decided that the matter is frivolous and vexatious, he proceeds to investigate the complaint and reaches a decision in relation thereto.

10. Counsel for the appellant has placed reliance on the terms of Council Directive 95/46/EC of October 24, 1995 on the protection of individuals with

regard to the processing of personal data and on the free movement of such data, and in particular art.28(1) thereof.

11. However, if one looks at the structure of art.28 of the Council Directive 95/46/EC, it does not seem to me that the provision to which the appellant has drawn attention is of any real assistance. Article 28(3) is in these terms:

> "3. Each authority shall in particular be endowed with:
> — investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;
> — effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;
> — the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.
> Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts."

12. It would seem that the complaint submitted by the appellant does not fit readily within the terms of art.28(3), but would seem to fit more naturally within the terms of art.28(4). It reads so far as material:

> "4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim."

13. In any event, I am quite satisfied that the effect of ss.10(1)(b)(i) and 26(1) when read together is quite clear and fully supports the conclusion reached in the Circuit Court.

14. Lest I be wrong in my conclusion that the Circuit Court did not have jurisdiction to entertain the appeal and in a situation where counsel on both sides have addressed the issues, I have decided to indicate a view on the substantive issue that the appellant had sought to canvass in his appeal.

15. Had an appeal been possible, it would then have been necessary to consider how a court should approach the hearing of an appeal from a body such as the Data Protection Commissioner. How a court should approach an appeal from a statutory body was addressed by Finnegan P. in the case of *Ulster Bank v Financial Services Ombudsman* [2006] IEHC 323; unreported, High Court, Finnegan P., November 1, 2006. In the course of his judgment he commented:

> "To succeed on this appeal the plaintiff must establish as a matter of probability that, taking the adjudicative process as a whole, the decision reached was vitiated by a serious and significant error or a series of such errors. In applying the test the court will have regard to the degree of expertise and specialist knowledge of the defendant. The deferential standard is that applied by Keane C.J. in *Orange v Director of Telecommunications Regulation* and not that in *State (Keegan) v Stardust Victims' Compensation Tribunal.*"

16. The reference by Finnegan P. to the standard applied by Keane C.J. in *Orange v Director Telecommunications Regulations* [2000] IESC 22; unreported, Supreme Court, May 18, 2000 was a reference to the following passage from the judgment of the Chief Justice in that case:

> "In short, the appeal provided for under this legislation was not intended to take the form of a re-examination from the beginning of the merits of the decision appealed from culminating, it may be, in the substitution by the High Court of its adjudication for that of the Director. It is accepted that, at the other end of the spectrum, the High Court is not solely confined to the issues which might arise if the decision of the Director was being challenged by way of judicial review. In the case of this legislation at least, an applicant will succeed in having the decision appealed from set aside where it establishes to the High Court as a matter of probability that, taking the adjudicative process as a whole, the decision reached was vitiated by a serious and significant error or a series of such errors. In arriving at a conclusion on that issue, the High Court will necessarily have regard to the degree of expertise and specialised knowledge available to the Director."

17. I am satisfied that the approach identified by Finnegan P. is the one that would have been appropriate to apply had an appeal been available. In particular, it seems to me that it would have been appropriate for the court to have regard to what Finnegan P. referred to as the deferential standard, when deciding whether to substitute its own view for that of the Data Protection Commissioner on the issue of whether an examination script constituted personal data. The Data Protection Commissioner is concerned with issues involving data protection on a daily basis. He is required to be in regular contact with his colleagues in other EU member states and is likely to be fully au fait with developments internationally. Pointing to the expertise of the Data Protection Commissioner does not mean that a court will abdicate its responsibilities and there may be cases where decisions of the Commissioner will be set aside, but if that happens, the decision to set aside the decision of the Commissioner will have been taken by a court that is conscious of the experience and expertise of the Commissioner. In this case, the Commissioner concluded that the examination script did not constitute personal data and accordingly, he was not in a position to identify any substantive breach of the Acts. He pointed out that there was no law in this jurisdiction to suggest it was personal data and in the course of a letter of July 21, 2010, pointed out

that there was no example of any other data protection authority within the EU considering such material to be personal data. In this case the script to which access is sought was a script created during an accountancy examination, an open book examination. While on its face the document would not contain any reference to Mr Peter Nowak and its author would be identified only by an examination number, it was of course potentially possible to link scripts to individual candidates. Obviously, if that were not so, there would be no point in setting the examination. However, little or no personal information about Mr Peter Nowak would be gleaned by anyone reading his script.

18. It seems to me that the conclusion arrived at by the Data Protection Commissioner was not one that would have come as a surprise to most people. The CAI had an examination system in place and one might have expected that Mr Nowak would have availed of that system. If he was unhappy with aspects of the system then there was scope available to him to challenge that system. However, what would have surprised most people was that instead of utilising the examination system to the full, Mr Nowak sought to invoke the data protection code in order to create a parallel examination code.

19. Accordingly, had it been possible to appeal to the Circuit Court, then, in my view, the court would have been correct to uphold the conclusion of the Data Protection Commissioner that the material in question did not amount to personal data within the meaning of the Acts and accordingly to dismiss the appeal. I am of that view notwithstanding that the applicant has pointed to the provisions of the equivalent British legislation and has drawn attention to the fact that schedule 7 of the Data Protection Act there, which contains a number of exemptions, lists examination scripts as an exempt category. Counsel for the applicant asks why it would be necessary to exempt examination scripts unless, in the absence of such a specific exemption, examination scripts would fall within the concept of personal data. It seems to me that that argument falsely assumes that all examination scripts fall to be treated in an identical manner. However, that is not necessarily so at all. The amount of personal information contained in an examination script may vary significantly depending on the nature of the examination. As the website of the respondent in its frequently asked questions section points out a psychometric test or IQ test would likely contain more information relating to the person that undertook the test than say a test of general knowledge. The examination that the applicant sat was, as we have seen, an "open book" examination. The applicant described the process involved in the course of a letter to the Commissioner dated July 14, 2010. He did so in these terms:

> "Since the above mentioned exam was an 'open book' exam I was able to reproduce answers provided during the real exam".

In the course of the written submissions on behalf of the respondent the point is

made that there was little more involved here than a transfer of model answers from text books into the examination booklet. Even if it was thought that there was an element of overstatement in that assertion, it does nonetheless provide a clear basis for the Commissioner to have formed the view that the examination script was not personal data.

20. Once the Commissioner had formed the view that the examination script did not constitute personal data it followed that he was being asked to proceed with an investigation where no breach of the Data Protection Acts could be identified. It was in those circumstances he had resort to s.10(1)(b)(i). That section refers to complaints that are frivolous or vexatious. However, I do not understand these terms to be necessarily pejorative. Frivolous, in this context does not mean only foolish or silly, but rather a complaint that was futile, or misconceived or hopeless in the sense that it was incapable of achieving the desired outcome, see *R. v North West Suffolk (Mildenhall) Magistrates' Court, ex p.Forest Heath District Council* [1997] EWCA Civ. 1575; unreported, Court of Appeal, May 16, 1997. Having regard to the view the Commissioner had formed that examination scripts did not constitute personal data, he was entitled to conclude that the complaint was futile, misconceived or hopeless in the sense that I have described, indeed such a conclusion was inevitable.

21. Having regard to the views that I have reached that Judge Linnane was correct that no appeal lay and to the views that I have reached on the arguments in relation to the merits of the case that have been canvassed, I propose to affirm the decision of the Circuit Court dated November 16, 2010.

Solicitors for the appellant: *Peter Connolly*
Solicitors for the respondent: *Philip Lee*

Gerard Nicholas Murphy
Barrister

[This decision is under appeal.]

131

4

THE HIGH COURT

[2013 No. 765JR]

BETWEEN/

MAXIMILLIAN SCHREMS

APPLICANT

AND

DATA PROTECTION COMMISSIONER (No.2)

RESPONDENT

JUDGMENT of Mr. Justice Gerard Hogan delivered on the 16th July, 2014

1. This is an application by notice of motion dated 26th June, 2014, on the part of Digital Rights Ireland Ltd. ("DRI") to be joined to the present judicial review proceedings as *amicus curiae*. This nature of this application cannot really be fully understood without reference to my earlier judgment which was delivered on 18th June, 2014, in respect of the substantive proceedings, *Schrems v. Data Protection Commissioner* [2014] IEHC 310. This judgment should accordingly be read in conjunction with that earlier judgment.

The background to the present proceedings

2. In these proceedings the applicant has challenged a decision of the Data Protection Commissioner not to investigate a complaint of his pursuant to s. 10(1)(b) of the Data Protection Act 1988 ("the 1988 Act"). The complaint was lodged following the revelations which a former US security contractor, Edward Snowden, made concerning the manner in which the US security authorities access personal data of non-US citizens on a mass and undifferentiated basis.

3. While the complaint was formerly directed at the major social network, Facebook (Ireland) Ltd., the gist of the objection does not really concern Facebook at all. The complaint was rather that in the light of the revelations made from May 2013 onwards by Edward Snowden concerning the activities of the US National Security Agency ("NSA"), there was no meaningful protection in US law and practice in respect of data so transferred to the US so far as State surveillance was concerned.

4. By letters dated 25th and 26th July, 2013, the Commissioner invoked his power under s. 10(1)(a) of the 1988 Act not to investigate this complaint further on the ground that this complaint was frivolous and vexatious, terms which in this case and in this particular statutory context simply mean that the Commissioner concluded that the claim was unsustainable in law.

5. The reason why the Commissioner reached this conclusion was because (i) there was no evidence that Mr. Schrems' personal data had been so accessed by the NSA (or other US security agencies)("the *locus standi* objection"), so that the complaint was purely hypothetical and speculative and (ii) because the European Commission had determined in its decision of 26th July 2000 (2000/520/EC)("the Safe Harbour Decision") that the United States "ensures an adequate level of [data] protection" in accordance with Article 25(6) of Directive 95/46/EC ("the 1995

Directive"). The Commissioner noted that the Safe Harbour decision was a "Community finding" for the purposes of s. 11(2)(a) of the 1988 Act, so that any question of the adequacy of data protection in that third country (in the present case, the United States) where the data is to be transferred was required by Irish law "to be determined in accordance with that finding." As this was the essence of the applicant's complaint – namely, that personal data was being transferred to another third country which did not in practice observe these standards – the Commissioner took the view that this question was foreclosed by the nature of the earlier Safe Harbour Decision.

6. In my judgment delivered on 18th June, 2014, (*Schrems v. Data Protection Commissioner* [2014] IEHC 310) I rejected the *locus standi* argument. I also found that mass and indiscriminate surveillance of communications, especially private communications generated within the home, would, as a matter of Irish law, be unconstitutional, having regard to the inter-action of the guarantees of privacy and Article 40.5.'s protection of the inviolability of the dwelling. That concept of inviolability would be wholly compromised if private communications of this kind generally made within the home were thus subjected to routine and undifferentiated surveillance by State agencies.

7. Section 11(1)(a) of the 1988 Act precludes the transfer of personal data to third countries, save where that third country "ensures an adequate level of protection for the privacy and the fundamental rights and freedoms" within the meaning of s. 11(1)(a) of the 1988 Act. I held that, were the matter judged entirely by Irish law, then measured by these constitutional standards and having regard to the (apparently) limited protection given to non-US data subjects by contemporary US law and practice so far as State surveillance is concerned, this would indeed have been a

matter which the Commissioner would have been obliged to investigate. It followed, accordingly, that if the matter were to be judged *solely* by reference to Irish constitutional law standards, the Commissioner could not properly have exercised his s. 10(1)(b) powers to conclude in a summary fashion that there was nothing further to investigate.

8. The parties were agreed, however, the matter is only partially governed by Irish law and that, in reality, on this key issue of the adequacy of data protection law and practice in third countries, Irish law has been pre-empted by general EU law in this area. This is because s. 11(2)(a) of the 1988 Act (as substituted by s. 12 of the Data Protection (Amendment) Act 2003) effects a *renvoi* of this wider question in favour of EU law. Specifically, s. 11(2)(a) of the 1988 Act provides that the Commissioner must determine the question of the adequacy of protection in the third State "in accordance" with a Community finding made by the European Commission pursuant to Article 25(6) of the 1995 Directive.

9. I then held (at paragraphs 64-70 of the judgment) that:

> "64. This brings us to the nub of the issue for the Commissioner. He is naturally bound by the terms of the 1995 Directive and by the 2000 Commission Decision. Furthermore, as the 2000 Decision amounts to a "Community finding" regarding the adequacy of data protection in the country to which the data is to be transferred, s. 11(2)(a) of the 1988 Act (as amended) requires that the question of the adequacy of data protection in the country where the data is to be so transferred "shall be determined in accordance with that finding." In this respect, s. 11(2)(a) of the 1988 Act faithfully follows the provisions of Article 25(6) of the 1995 Directive.

65. All of this means that the Commissioner cannot arrive at a finding inconsistent with that Community finding, so that if, for example, the Community finding is to the effect that a particular third party state has adequate and effective data protection laws, the Commissioner cannot conclude to the contrary. The Community finding in question was, as we have already seen, to the effect that the US does provide adequate data protection for data subjects in respect of data handled or processed by firms (such as Facebook Ireland and Facebook) which operate the Safe Harbour regime

66. It follows, therefore, that if the Commissioner cannot look beyond the European Commission's Safe Harbour Decision of July 2000, then it is clear that the present application for judicial review must fail. This is because, at the risk of repetition, the Commission has decided that the US provides an adequate level of data protection and, as we have just seen, s. 11(2)(a) of the 1998 Act (which in turn follows the provisions of Article 25(6) of the 1995 Directive) ties the Commissioner to the Commission's finding. In those circumstances, any complaint to the Commissioner concerning the transfer of personal data by Facebook Ireland (or, indeed, Facebook) to the US on the ground that US data protection was inadequate would be doomed to fail.

67. This finding of the Commission is doubtless still true at the level of consumer protection, but, as we have just seen, much has happened in the interval since July 2000. The developments include the enhanced threat to national and international security posed by rogue States, terrorist groupings and organised crime, disclosures regarding mass and undifferentiated surveillance of personal data by the US security authorities, the advent

of social media and, not least from a legal perspective, the enhanced protection for personal data now contained in Article 8 of the Charter.

68. While the applicant maintains that the Commissioner has not adhered to the requirements of EU law in holding that the complaint was unsustainable in law, the opposite is in truth the case. The Commissioner has rather demonstrated scrupulous steadfastness to the letter of the 1995 Directive and the 2000 Decision.

69. The applicant's objection is, in reality, to the terms of the Safe Harbour Regime itself rather than to the manner in which the Commissioner has actually applied the Safe Harbour Regime. There is, perhaps, much to be said for the argument that the Safe Harbour Regime has been overtaken by events. The Snowden revelations may be thought to have exposed gaping holes in contemporary US data protection practice and the subsequent entry into force of Article 8 of the Charter suggests that a re-evaluation of how the 1995 Directive and 2000 Decision should be interpreted in practice may be necessary. It must be again stressed, however, that neither the validity of the 1995 Directive nor the validity of the Commission's Safe Harbour decision have, as such, been challenged in these proceedings.70. Although the validity of the 2000 Decision has not been directly challenged, the essential question which arises for consideration is whether, *as a matter of European Union law*, the Commissioner is nonetheless absolutely bound by that finding of the European Commission as manifested in the 2000 Decision in relation to the adequacy of data protection in the law and practice of the United States having regard in particular *to the subsequent entry into force of Article 8 of the Charter*, the provisions of Article 25(6) of the 1995 Directive notwithstanding.

For the reasons which I have already stated, it seems to me that unless this question is answered in a manner which enables the Commissioner either to look behind that Community finding or otherwise disregard it, the applicant's complaint both before the Commissioner and in these judicial review proceedings must accordingly fail."

Given that the critical issue in the present case was whether US law and practice afforded sufficient data protection and that no issue was ever raised in these proceedings concerning the actions of Facebook Ireland/Facebook *as such*, I took the view that the real question was whether the Commissioner was bound by the earlier findings to this effect by the European Commission in the Safe Harbour Decision. In other words, this was really a complaint concerning *the terms* of that decision, rather than the manner in which the Commissioner *had applied it*: see paragraph 69 of the judgment. While it is true that Article 3(b) of the Safe Harbour Decision allows the national authorities to direct an entity to suspend data flows to that third country, this is in circumstances where - unlike the present case - the complaint is in substance directed to *the conduct of that entity*. Here the real objection is not to the conduct of Facebook *as such*, but rather to the fact that the Commission has already determined that the US law and practice provides adequate data protection in circumstances where it is clear from the Snowden disclosures that personal data of EU citizens so transferred to the US can be accessed by the US authorities on a mass and undifferentiated basis, thus permitting the physical transfer of such data from Ireland 9and elsewhere in the European Union) to the United States."

10. It must be stressed that neither the validity of the 1995 Directive nor the 2000 Safe Harbour decision were, as such, challenged in these proceedings, a factor which, as we shall later see, has relevance to the present application. Nor has it been suggested that s. 11(2)(a) of the 1988 Act (as amended) does not faithfully reflect the terms of Article 25(6) of the 1995 Directive or that it was otherwise contrary to EU law.

11. In these circumstances I took the view that it would be appropriate that I should refer the question of whether, having regard in particular to my earlier findings of fact regarding the Snowden disclosures and the subsequent entry into force of Article 7 and Article 8 of the Charter and the recent judgment of the Court of Justice in Case C-293/12 *Digital Rights Ireland* [2014] E.C.R. I-000, the Commissioner was bound by the earlier determination of the European Commission in the Safe Harbour Decision as to the adequacy of the data protection offered by US law and practice.

12. So far as the present application is concerned, two separate issues arise. First, should DRI be joined as an *amicus curiae* to the present proceedings? Second, even if it were to be so joined, should it be permitted to have an additional question or questions added to the proceedings? We may now consider these issues in turn.

Should DRI be joined as an *amicus curiae?*

13. The jurisdiction of the High Court and Supreme Court to permit a third party to be joined as an *amicus* was adumbrated by Keane C.J. in *I. v. Minister for Justice, Equality and Law Reform* [2003] IESC 42, [2003] 3 I.R. 197 where he stated ([2003] 3 I.R. 197, 203-204):

> "While there are no statutory provisions or rules of court providing for the appointment of an *amicus curiae,* save in the case of the Human Rights

Commission, the court is satisfied that it does have an inherent jurisdiction to appoint an *amicus curiae* where it appears that this might be of assistance in determining an issue before the court. It is an unavoidable disadvantage of the adversarial system of litigation in common law jurisdictions that the courts are, almost invariably, confined in their consideration of the case to the submissions and other materials, such as relevant authorities, which the parties elect to place before the court. Since the resources of the court itself in this context are necessarily limited, there may be cases in which it would be advantageous to have the written and oral submissions of a party with a *bona fide* interest in the issue before the court which cannot be characterised as a meddlesome busy body. As the experience in other common law jurisdictions demonstrates, such an intervention is particularly appropriate at the national appellate level in cases with a public law dimension.

It is, at the same time, a jurisdiction which should be sparingly exercised. Clearly, the assistance to be given to an appellate court will be confined to legal arguments and supporting materials. It is not necessary to consider the circumstances in which it would be appropriate for the High Court to appoint an *amicus curiae*. It is sufficient to say that, as was pointed out in *United States Tobacco Company v. Minister for Consumer Affairs* (1988) 83 ALR 79 the position of an *amicus curiae* is quite different from that of an intervener. It was said in that case that an *amicus curiae*, unlike an intervener, has no right of appeal and is not normally entitled to adduce any evidence.

In the present case, an issue of public law arises and the judgment of the court may affect parties other than those now before the court. The court was

satisfied that the UNHCR might be in a position to assist the court by making written and oral submissions on the question of law certified by the High Court and, accordingly, appointed it to act as *amicus curiae* and, for that purpose, to make oral and written submissions."

14. The law has admittedly moved on to some degree in the interval. Specifically, the jurisdiction of the High Court to appoint an *amicus* in an appropriate case has been recognised: see, *e.g., O'Brien v. Personal Injuries Compensation Board* [2005] 3 I.R. 328. Yet the basic parameters of the jurisdiction to appoint an *amicus* remain those as expounded by Keane C.J. In essence, the court will appoint an *amicus* only where it is satisfied that that putative party will be in a position to assist the court in respect of the legal issues which arise within the scope of the proceedings as defined by the parties, often by availing of the peculiar expertise or insight at its disposal. This was accordingly the case in respect of the UNHCR in an important refugee case in *I.* and the same could be said of the Law Society in *O'Brien* in a significant case with implications for the solicitor/client relationship.

15. In this regard, the neutrality of the putative *amicus* is also a factor, since as Clarke J. observed in *Fitzpatrick v. FK (No.1)* [2007] 1 I.R. 406, 415, one of the important factors to be taken into account is whether:

"the proposed *amicus* might reasonably be said to be partisan or, on the other hand, to be largely neutral and in a position to bring to bear expertise in respect of an area which might not otherwise be available to the court."

16. The underlying issue in *Fitzpatrick* concerned the legality of the administration of a blood transfusion following a massive post-partum haemorrhage to a patient who had falsely represented herself to the maternity hospital which was treating her up to that point to be a Roman Catholic. It was only when gravely ill

following the delivery of a child that she later claimed to be a member of Jehovah Witnesses and refused to give her consent to a blood transfusion. A company which represented the interests of the Witnesses, the Watch Tower Bible and Tract Society of Ireland, sought to be joined as an *amicus* to the litigation, but this was refused by Clarke J. on the basis that it "would adopt a partisan approach which is unlikely to differ from that likely to be adopted" from that of the patient herself.

17. It is also significant that in *O'Brien* Finnegan P. stressed that the Law Society "has not just a sectional interest, that is the interest of its members, but a general interest which should be respected and to which regard should be had": see [2005] 3 I.R. 328, 333. That case raised wider questions regarding the solicitor/client relationship in the context of personal injuries claims and to that extent the Law Society had an important contribution to make to draw attention to the implications and importance of that relationship.

18. It is also clear that the *amicus* does not have the status of a party to the litigation – so that, for example, it cannot call evidence or lodge an appeal - and it cannot add materially to the costs of the litigation by, for example, seeking its own costs. The case must furthermore normally involve questions of public law, often with significant implications for the general public. Moreover, as Keane C.J. stressed in I., the jurisdiction is one to be "sparingly exercised." Measured, then, by these standards, should, then, the Court appoint DRI as an *amicus*?

Costs

19. Turning first to the issue of costs it is clear from the very terms of the motion papers filed by DRI that it seeks an order directing that it should bear its own costs. It is accordingly clear that if it is joined as an *amicus* this fact will not in itself have any material implications for the costs of the applicant and the respondent.

Whether the case involves questions of public law with significant implications for the general public

20. There is no question but that this case involves questions of public law concerning the scope and extent of data protection which are of significant national and, indeed, international importance. This criterion is accordingly plainly satisfied.

The expertise of DRI

21. The expertise of DRI in all matters concerning the internet, the information society and data protection does not appear to be in doubt. Indeed, in his affidavit in support of the application, Antóin Ó Lachtnáin, a director of DRI, states that DRI:-

> "operates a website...designed to facilitate information about the various civil, legal and human rights that arise in the judicial age...the applicant has also sought to inform public debate through other means, including newspaper articles, meetings with elected representatives, submissions to official bodies and the organising of public events on issues such as privacy and copyright reform. The applicant has made submissions to the Oireachtas Joint Committee on Transport and Communications hearings on social media and has made a joint submission with Catherine Murphy T.D. and Stephen Donnelly T.D. and McGarr Solicitors to the Government's Copyright Review Committee...I say that the applicant is a *bona fide* organisation with credibility and a track record of success in forming public debate and assisting with vindicating the rights of the general public on the internet and within the information society."

22. It is also significant that in *Digital Rights Ireland Ltd. v. Minister for Communications* [2010] IEHC 221, [2010] 3 I.R. 251, 292 McKechnie J. recognised

that in those proceedings – which involved a challenge to the validity of the Data Retention Directive - the company "was acting *bona fide* and is neither being a crank, meddlesome or vexatious." Nor can I ignore the fact that the Court of Justice ultimately held following an Article 267 TFEU reference from this Court that the Data Retention Directive was itself invalid: see Case C-293/12 *Digital Rights Ireland Ltd.*[2014] E.C.R. I-000.

Whether DRI has been assigned any role by either domestic or international law in the area which is the subject matter of the litigation

23. In all (or, at least, virtually all) of the cases in which an *amicus* has been appointed by an Irish court the *amicus* has been assigned an important role in relation to the subject matter of the litigation by either national or international law. This was true of the UNHCR in *I*, the Law Society in *O'Brien* and the Equality Authority in *Doherty v. South Dublin County Council* [2006] IESC 57, [2007] 1 I.R. 246 (a case concerning the rights of members of the travelling community). Conversely, the fact that DRI have been given no such public role in relation to copyright matters was a factor which weighed heavily with Kelly J. in his judgment in *EMI Records (Ireland) Ltd. v. UPC Communications Ireland Ltd.* [2013] IEHC 204 where he refused to make such an order in a case involving the application of the same applicant, DRI, to be joined as a party to litigation involving copyright and internet piracy.

24. At the same time I think that it clear from the case-law that the fact that the putative *amicus* has been given no such express role by domestic or international law cannot *in itself* be regarded as a disqualifying factor. Thus, for example, in *Fitzpatrick* Clarke J. contemplated that the Watch Tower Bible and Tract Society of Ireland might successfully apply to be made an *amicus* at a later stage of those proceedings were the circumstances so to warrant it. This was also the approach taken by Kelly J. in *EMI*

when he stated that he did not regard the fact that DRI had been given no such public role as a threshold factor which justified the refusal of the *amicus* application *in limine.* It was, rather a discretionary factor which was nonetheless of "some significance".

Whether the applicant might be expected to adopt a partisan fashion were it to be appointed as an *amicus.*

25. It is clear that the courts will be at least disinclined to appoint as an *amicus* a party that might be expected to act in a partisan fashion. This was the case in *Fitzpatrick* where the applicant "did not suggest that it would not adopt a partisan position": see [2007] 1 I.R. 406, 417, *per* Clarke J. Similar views were also expressed in *EMI* where Kelly J. emphasised the fact that DRI had engaged in a public campaign directed against the introduction of a statutory instrument dealing with copyright infringement and internet piracy in proceedings which concerned these very issues. The very fact that the evidence showed that DRI would not act in a neutral fashion in relation to these matters was a factor which weighed heavily against its appointment as an *amicus*.

26. There is, however, no suggestion that DRI have been involved in any public campaigns in relation to the issues raised by this litigation. Mr. Ó Lachtnáin has, moreover, averred in his affidavit grounding the present motion that DRI "is concerned to take no position of partisanship in respect of the dispute between the parties here."

27. One cannot help feeling, however, that on this question of partisanship both litigants and courts have all at times engaged in something of a polite fiction. After all, the views of the UNHCR regarding the plight of refugees are well known. The Law Society can be expected to have strong views on the rights of solicitors and their

clients. One may equally assume that DRI has strong views on the adequacy of the Safe Harbour regime.

28. Partisanship cannot, moreover, be easily measured by objective standards. This is perhaps especially true of legal proceedings where, after all, the task of the advocate is to persuade. The submission which aspires to complete impartiality and icy detachment may be regarded by some on this account as bland and ineffective.

29. What is, I think, clear from the views of Kelly J. in *EMI* is that open partisanship which is detached from the underlying legal materials and the legal merits is most undesirable and attracts judicial disapproval. In that respect, therefore, the legal advisers representing the *amicus* bear a particular responsibility to ensure that the standards appropriate to legal professionals are not compromised in any written or oral legal submissions made on behalf of the *amicus*, even if those submissions are strongly advanced in favour of a particular legal argument. One of those duties of counsel is, of course, to bring all relevant legal materials and authorities to the attention of the court, even if those materials are adverse to the interests of the client.

30. All of this is to say that is that while prospective *amicii* who hold strong institutional views on the subject matter of the dispute are not disqualified on that account alone from being appointed as an *amicus,* they are also expected and required to confine themselves to the traditional parameters of legal argument. In view of Mr. Ó Lachtnáin's unchallenged averments regard DRI's likely role, I am prepared to assume in its favour that it will be abide by these strictures.

The attitude of the parties

31. Finally, the view of the actual parties to the litigation regarding the application of DRI to be joined as an *amicus* is a most important consideration. The

Commissioner has taken a neutral view, although his counsel, Mr. McDermott, has drawn my attention to the relevant case-law, including the comments of Kelly J. in *EMI* regarding the role of DRI in respect of the dispute in those proceedings.

32. The applicant himself, Mr. Schrems, is opposed to the joinder of DRI as an *amicus*. His counsel, Mr. O'Shea, makes the point that all relevant arguments are likely to be canvassed given the large number of Member States who, it is anticipated, are likely to intervene before the Court of Justice. The applicant is a postgraduate law student in his twenties who is at the start of his legal career. He is naturally and understandably concerned about the possible costs implications of the joinder of another party.

33. So far as the costs are concerned, it will, however, be a condition of any joinder that DRI will not be allowed to seek costs from any party. In fairness, DRI have at all times recognised this limitation. It may, furthermore, be anticipated that its participation in oral argument will be confined to a short period of time, so that its participation in the proceedings will not represent an additional costs burden for either party by adding appreciably to the length of the hearing.

34. I agree with Mr. O'Shea that it is very likely that many Member States are likely to seek to intervene in the Article 267 TFEU reference, so that it is unlikely that any relevant point will be overlooked. Yet given the track record of DRI – not least its recent successful challenge to the validity of the Data Retention Directive – it is likely that it will be in a position to articulate its own distinctive views on these questions of data protection and surveillance. The articulation of these views may assist the Court of Justice as that Court grapples with these difficult questions.

Conclusions on whether DRI should be appointed an *amicus*

35. I confess that the application of these principles is not straightforward. The opposition of the applicant to the joinder of DRI and the fact that it has no legally conferred role in matters of data protection are factors which tell against the making of such an order. The comments of Kelly J. in *EMI* regarding the conduct of DRI in relation to the issues of copyright privacy which arose in that case also weigh heavily with me.

36. Yet, not without considerable hesitation, I have concluded that I should make such an order appointing DRI as an *amicus*. I take this view because in the light of the decision of the Court of Justice in *Digital Rights Ireland*, I think that DRI can articulate its own distinctive view which may possibly assist the Court in respect of these difficult and troubling questions which are the subject of the reference.

Whether DRI should be permitted to add an additional question to the questions already referred pursuant to Article 267 TFEU

37. There remains for consideration the question of whether DRI should be permitted to include an additional question on the reference. DRI urge that I should also refer the questions of the validity of the 1995 Directive and the Safe Harbour Decision itself to the Court of Justice.

38. As I indicated at the hearing, I did not think that this course of action would be appropriate. As I was at pains to stress in the first judgment, the applicant has never chosen to challenge the validity of either the Directive or the Safe Harbour decision. Quite apart from the fact that - as decisions such as *I.* illustrate - an *amicus* is normally bound by the parameters of the existing litigation, the addition of these questions would radically change the nature of the proceedings. Moreover, given that, as I have found, s. 11(2)(a) of the 1988 Act gives effect to the requirements of Article 25(6) of the 1995 Directive by obliging the Commissioner to follow the terms of the

Safe Harbour Decision, a challenge to the validity of the Directive would be tantamount to a challenge to the constitutionality of s. 11(2)(a).

39. On any view, the Attorney General would have to be party to any proceedings in which the validity of the 1995 Directive was put at issue. Inasmuch as this would also amount in substance to a challenge to the constitutionality of s. 11(2)(a) – given that, on this argument, the Oireachtas would have wrongly transposed an item of Union legislation which was itself later found to be invalid by the Court of Justice – Order 60, r.1 of the Rules of the Superior Courts, 1986 requires that the Attorney General be joined as a party. Yet she was never served with the proceedings or joined as a party to the present proceedings.

40. It is, of course, true to observe that as counsel for DRI, Mr. Crehan, observed, there have been instances in the past where an *amicus* can formulate questions or suggest changes to draft questions in the context of a pending Article 267 TFEU reference. Mr. Crehan pointed to the fact that in *Digital Rights Ireland,* counsel for the *amicus* in that case – namely, the Irish Human Rights Commission – made suggestions of this kind.

41. Yet what is proposed here is appreciably different, given that it would radically change the nature of the proceedings and would involve the additional delay and costs associated with the joinder of a further party, namely, the Attorney General. These additional questions would effectively make DRI a party to the litigation in order to facilitate it to make a case which the parties themselves had never made.

42. For all of these reasons, I would not permit DRI as *amicus* to expand the scope of the proceedings or to alter the nature of the questions which I have already proposed should be transmitted to the Court of Justice.

Conclusions

43. In summary, therefore, I have concluded - albeit not without hesitation – that I should join DRI as an *amicus* to the present proceedings. I will not, however, permit DRI to add additional questions to the Article 267 TEU reference, as the proposed questions would radically alter the nature and scope of the existing proceedings and would require the joinder of a further additional party (namely, the Attorney General), thereby involving further additional costs and delay.

Approved

[redacted]

15th July 2014

5

Data Protection Law and Practice

Fourth Edition

Rosemary Jay

SWEET & MAXWELL

THOMSON REUTERS

157

F DATA PROCESSORS

July 2, 1998:

CHAPTER 8

Overseas Or Cross-Border Transfers Of Personal Data

William Malcolm

INTRODUCTION

The aim of the relevant provisions on cross-border flows of personal data in the Directive is to ensure that personal data transferred outside the EEA countries are handled in accordance with the data protection principles. The transfer of personal data outside the EEA is prohibited, save for those cases where the exceptions or derogations can be claimed, unless the destination country (which is also taken to include the country of eventual destination if more than one data movement is contemplated) has an adequate level of personal data protection.[1] Although the derogations seem reasonably wide, they cannot be used in all cases. Some data controllers (particularly international businesses) have long expressed concerns that the exceptions and derogations are inflexible and bureaucratic. This has been the source of continued friction since the Directive was passed and is now a source of intensifying debate as businesses across the EU look to adopt cloud based services and as the EU Commission looks to reform the Directive. Indeed the "location of data processing" was one of the key themes of the July 2012 Opinion of the Working Party on Cloud Computing,[2] which acknowledged that "...the traditional legal instruments providing a framework to regulate data transfers to non-EU third countries not providing adequate protection, have limitations"[3] in a cloud context. Some have expressed concern that some Member States have taken too relaxed a view of the prohibition and regulatory authorities in at least one jurisdiction have been challenged before the courts for taking too strict a view of the rules banning transfers.[4] In non-EEA countries the provision has been seen as a way for Brussels to extend the impact of the Directive beyond the borders of the EU and ensure that others adopt a system of regulation similar to the EU model. **8–01**

The Commission has the capacity to make findings of adequacy in relation to third countries. The standard it has applied for making such findings in respect of a country is that the country has generally applicable law equivalent to EU regimes. In respect of the United States, although there has been no general finding of adequacy, Safe Harbor has made transfers possible to a limited number

[1] Dir.95/46 art.25.1.

[2] Working Party Opinion 05/2012 on Cloud Computing 01037/12/EN WP 196 July 2012.

[3] Ref.2, p.17.

[4] [Reference case against Spanish data protection supervisory authority].

152

of organisations that have agreed to meet standards similar to those found in the Directive. The "Safe Harbor" agreement with the US reached in July 2000 came into effect in November 2000. This only applies to certain US organisations; there is no concept of a Safe Harbor in any other jurisdiction.

Another possible solution to the problems caused by the approach of the Directive to overseas transfers is the adoption of contractual solutions. Contracts have long been considered as potential vehicles to deliver data protection solutions. Work was carried out on contracts by the Council of Europe in the 1980s and has continued, with an increasing degree of sophistication, ever since; although some still argue that the current contractual standards are not fit for the modern cloud based environment.

8–02 A further possible route to enable transfers to countries without adequate protection is the development of Binding Corporate Rules (BCRs), under which a global company is empowered to establish its own scheme of binding internal contracts which commit the organisation to adhere to an appropriate data protection standard. The scope of BCRs has been extended recently to include processers and the mutual recognition procedure covering most of the EU has made adoption faster. However, notwithstanding these developments, take up of BCRs has been somewhat limited in the context of the overall volume of international data transfers and some question whether this solution (which requires heavy input from national supervisory authorities) is scalable for the modern cloud. Despite these concerns, BCRS are, at the time of writing, being touted as a central plank of future data protection law reform in this area.

8–03 A fundamental difference in attitudes to overseas transfers between the approach of regulators and the pragmatism of business has gradually emerged since 1998. The Directive (and hence the laws of all Member States) allows the export of data where one of the derogations apply. Therefore businesses tend, not unreasonably, to consider the possibility of using one or more of the derogations as the first option when faced with a transfer to a non-EEA country with no finding of adequacy. Generally, it is only if none of the derogations apply, that businesses look to whether contracts, Safe Harbor or BCRs, or a combination of such measures, offer an acceptable solution. Regulators, on the other hand, are keen to emphasise that derogations should be the last option and only relied upon where no way of providing adequate protection can be found.

8–04 SUMMARY OF THE MAIN POINTS

a) The eighth data protection principle[5] provides that:

> "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

b) The interpretation provisions for the eighth principle[6] provide an interpretation of the phrase "adequate level of protection".

[5] As set out in Sch.1 Pt 1 para.8 of the 1998 Act.
[6] As set out in paras 13–15 of Pt 2 of Sch.1 para.13.

153

nilar to those found in the
eached in July 2000 came
ain US organisations; there
n.
l by the approach of the
actual solutions. Contracts
o deliver data protection
Council of Europe in the
sophistication, ever since;
tandards are not fit for the

ountries without adequate
les (BCRs), under which a
cheme of binding internal
e to an appropriate data
tended recently to include
ering most of the EU has
developments, take up of
of the overall volume of
ther this solution (which
orities) is scalable for the
th of writing, being
reform in this area.
as transfers between the
ss has gradually emerged
Member States) allows the
refore businesses tend, not
or more of the derogations
non-EEA country with no
the derogations apply, that
BCRs, or a combination of
ors, on the other hand, are
option and only relied upon
e found.

or territory outside the
nsures an adequate
ects in relation to the

ple[6] provide an

c) There are a number of exemptions[7] to the restriction in the eighth principle.
d) Where a "Community finding" has been made in relation to a particular kind of transfer then any question as to an "adequate level of protection" must be determined in accordance with that finding.
A "Community finding" is a finding of the European Commission,[8] that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Art.25(2) of the Directive.
e) Transfers to non-EEA countries are included on the data controller's register of notification, but this can be done in very general terms.
f) A transfer is a processing operation in itself and the data controller must also be able to rely on one of the grounds for processing in order to validate any overseas transfer.
g) Failure to comply with the principle is not an offence but may be subject to enforcement action by the Commissioner.
h) As well as complying with the eighth principle an overseas transfer must comply with the other principles and issues of fairness, transparency, lawfulness and security of the transfer must be considered.
i) Common ways for business to comply with the rules on international transfers include use of Model Contractual Clauses (MCCs), Safe Harbor (for transfers to certain US companies), BCRs or transfer to a country "approved by the EU Commission".

WHAT IS A CROSS-BORDER DATA TRANSFER?

No definition of a transfer is provided in the Directive or the 1998 Act. Clause 1 of the Data Protection Bill contained a definition of what constitutes a transfer, but the proposed definition did not survive into the final Act. The clause would have provided that:

> "A person who:
>
> a) discloses data to a person in a country or territory; or
> b) otherwise makes the information contained in the data available to a person in a country or territory,
>
> is taken to transfer the data to that country or territory."

This was a broad definition of a "transfer". It would clearly have covered personal data being communicated over the telephone (the "push" transfer) and might have been wide enough to cover the provision of access rights to a third party outside the EEA or placing of material on a website which would potentially be available to persons outside the EEA (the "pull" transfer).

The definition was dropped during consideration of the Bill. In the absence of such a definition it was not clear whether personal data made available for access or posted on an Internet site from where it could be accessed would involve a

[7] Para.14 contains a reference to Sch.4 to the 1998 Act.
[8] Under the procedure provided for in art.31(2) of the Data Protection Directive.

154

transfer outside the EEA. However, the point was decided by the European Court in the *Lindqvist*[9] case, resulting in the decision that the former clearly is a transfer but the later will not necessarily be and may depend on where the server used is situated. The Guide available from the Office of the Information Commissioner[10] distinguishes between transfer and transit as follows:

> "A transfer is not the same as transit of information through a country. The eighth principle will apply only if the information moves to a country, rather than simply passing through en route to its destination".

The Act provides that the transfer of information in a form in which it would not fall under the UK Act, for example on a paper copy outside the definition of a "relevant filing system", which is intended to be held as data in the overseas jurisdiction, will still be regarded as a transfer.[11]

A data controller may still retain control over the relevant personal data even if it (or a copy) has been transferred overseas. Control may, for example, be retained by way of strict contractual terms between a transferor and transferee.

8–05 In *Lindqvist*,[12] Mrs Lindqvist had placed personal data on to a website which was hosted within the EEA. The European Court decided that she had not transferred personal data outside the EEA. There is no transfer to a third country within the meaning of art.25 of the Directive in such circumstances, notwithstanding that it thereby makes the data accessible to anyone who connects to the internet, including people in a third country.[13] The Court explained that, if the Directive were interpreted to mean that there was a transfer whenever personal data were loaded on to a website that could be accessed over the internet, then if the Commission found that even one country did not have adequate protection the Member States would be obliged to prevent any personal data being placed on the internet.

This leaves open the question of who is responsible for the "transfer" when such personal data are accessed from a non-EEA. The UK Commissioner has considered the intention of the person uploading the data to be a material consideration:

> "Putting personal data on a website will often result in transfers to countries outside the EEA. The transfers will take place when someone outside the EEA accesses the website. If you load information onto a server based in the UK so that it can be accessed through a website, you should consider the likelihood that a transfer may take place and whether that would be fair for the individuals concerned. If you intend information on the website to be accessed outside the EEA, then this is a transfer".[14]

While the decision in *Lindqvist* is wholly understandable, it leaves a possible lacunae in control. As noted from the quotation above the Commissioner seeks to deal with this by pointing out that, even where there is no intention to transfer, the

---

[9] See Ch.3 for a full explanation of the case.
[10] The Guide to Data Protection.
[11] DPA s.1(3).
[12] *Lindqvist* ECJ Case C – 101/01.
[13] Ref.10.
[14] Ref.10.

155

very fact that the data controller has made the data so widely accessible raises the question of whether the processing is fair.

Onward transfers

The Directive does not deal specifically with onward transfers. It simply requires that one of the elements to be taken into consideration when determining adequacy is the "country of final destination", a phrase which is repeated in the UK provision.[15] The question of how far the recipient organisation in a third country is able to make further transfers and to what extent the original exporting data controller should be held responsible for such transfers is an unresolved question. As might be anticipated, the Working Party and the Commission have been quick to emphasise to data controllers that, in the view of the Working Party and Commission, the onward transfers of personal data to recipients outside the EEA are equally governed by the prohibitions on transfer. **8–06**

Adequate protection

The core of the provisions relating to cross-border transfers is the assessment as to whether the foreign country offers an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Guidance on assessing whether a foreign country offers adequate protection has been produced by the Article 29 Working Group and the UK Commissioner.[16] In this chapter the guidance from those sources is considered but, however persuasive such guidance may be, it is not in itself law.

Provisions in the Act

The Act itself sets out a number of criteria in Sch.1 Pt 2 para.13 to which any data controller must have particular regard in assessing adequacy. **8–07**

The first of these criteria requires a data controller to have regard to the nature of the data. The clear implication here is that there will be more or less sensitive data (sensitive both in the sense defined by the Act as well as in its more general meaning), which will require correspondingly more or less protection. This is, of course, a parallel of the provision in the interpretation of the seventh principle on security measures which requires consideration to be given to the nature of the data to be protected in assessing the "appropriateness" (as opposed to "adequacy") of the relevant security system. It is interesting that the two sets of interpretative provisions on two consecutive principles should utilise two different concepts—"appropriateness" and "adequacy". It is submitted that the concept of "adequacy" could easily have been utilised in both sets of provisions and would have provided thereby at least the security of familiarity.

---

[15] DPA Sch.1 Pt II para.13.

[16] See ICO website section on Sending Personal Data Outside the EEA. The topic is covered in the Guide to Data Protection and four specific notes on Assessing Adequacy, Model Contract Clauses, Binding Corporate Rules and Outsourcing. These have replaced the Commissioner's earlier Guidance.

158

No further guidance is given in the legislation as to how "adequacy" needs to be balanced against the nature of the data, but clearly the minimum requirement is for a data controller to be able to show a rational decision-making process along the lines of,

> "I considered the level of protection, which involves A, B and C, to be offered by country M to be adequate, given that the data we transferred contained details of X, Y and Z."

The second and third criteria to be considered are the country or territory of origin of the information contained in the data and the country and territory of final destination.

8–08 The implication seems to be that if data were gathered in a country with an "inadequate" system of data protection then a transfer to a country with a similarly inadequate system might be acceptable or at least transfer back to the country of origin. The fourth criterion requires consideration to be given to the purposes for which and the period during which the data are intended to be processed. This is a consideration which goes hand in hand with the requirement that, in assessing adequacy, regard must be had to the nature of the data. A data controller thus must look not only at the nature of the data to be processed but also at the nature of the processing to be carried out in the foreign territory or country and the time when that processing is planned to take place.

Thus the controller will ask the following questions:

(a) What is the nature of the data?
(b) What will be done with it?
(c) For how long will it be used?

Again no further guidance is given in the legislation as to what types of processing will require more or less protective regimes. But, as with the criteria obliging consideration of the nature of the data, it is submitted that the data controller must be able to demonstrate a rational decision-making which takes into account all these factors.

The fifth to eighth criteria require a data controller to consider the details of the data protection regime or regimes in place in the country of destination and specifically:

(a) the law in force;
(b) the international obligations adhered to;
(c) relevant enforceable codes of conduct or other rules; and
(d) security measures taken in respect of the data.

The last provision requires the data controller to consider what security measures are to be taken with respect to the specific data to be transferred, whereas the first three require consideration to be given to the generality of the regimes in place.

The eighth principle commences by stating that:

157

"An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to . . . ",

before reciting the eight criteria to be considered. Thus the eight criteria are not exhaustive of the matters which a data controller may have to consider in assessing adequacy.

Adequacy assessment

Help in assessing adequacy has already been provided at both an EU level and at a national level. **8–09**

EU level

At the EU level there have been a number of formal decisions as to countries and territories which offer an adequate level of protection.[17] The decisions are "Community findings" under the Directive. The interpretative provisions on the eighth principle specifically provide for "Community findings" to be taken into account in deciding adequacy.[18] Such findings on particular types of transfer are binding on data controllers and the national data protection enforcement agencies. A "Community finding" is defined as a finding of the European Commission, under the procedure provided for in art.31(2) of the Data Protection Directive, that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of art.25(2) of the Directive.[19] The decisions have been issued as Commission Decisions which operate as Community legal instruments and are directly applicable without the need for further implementing provisions however the UK has chosen to have a formal adoption mechanism. **8–10**

The Commission is also empowered to decide that certain standard contractual clauses offer sufficient safeguards in relation to transfers to countries with data protection regimes providing otherwise inadequate protection[20]. This is discussed more fully below.

Article 29 Paper

The Article 29 Working Party[21] produced some helpful guidance on the interpretation of arts 25 and 26 of the EU Directive (the Articles covering cross-border transfers)[22] in July 1998, which has subsequently been relevant in making adequacy assessments and is referred to in later Commission decisions.[23] Although the Working Party has issued a wide range of opinions on international **8–11**

[17] See *http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm* [Accessed September 16, 2012] for a full list.
[18] DPA Sch.1 Pt 2 para.15.
[19] For an explanation of the art.31 procedure, see Ch.10.
[20] The Directive art.26 paras 2–4.
[21] See Ch.23 for the constitution and work of the Article 29 Working Party.
[22] "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" DG XV D/5025/98.
[23] See recital 3 of Council Decision 2001/497/EC.

158

transfer issues, this paper remains the only paper covering the full framework of arts 25 and 26. It is also the most helpful and significant.

The guidance suggests that any meaningful analysis of "adequate protection" must comprise two basic elements: an assessment of the content of the rules applicable and an assessment of the means for ensuring their effective application.

The Working Party also submits that:

> "Using Directive 95/46/EC as a starting point, and bearing in mind the provisions of other international data protection texts, it should be possible to arrive at a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements compliance with which could be seen as a minimum requirement for protection to be considered adequate."

Those principles and requirements, the Working Party suggests, are as follows.

Content Principles

8–12 The basic principles to be included are the following:

(a) The purpose limitation principle—data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in art.13 of the Directive.[24]

(b) The data quality and proportionality principle—data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

(c) The transparency principle—individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with arts 11(2)21 and 13 of the Directive.

(d) The security principle—technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

(e) The rights of access, rectification and opposition—the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to

[24] Art.13 permits a restriction to the "purpose principle" if such a restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest, or the protection of the data subject or the rights and freedoms of others.

the processing of the data relating to him/her. The only exemptions to these rights should be in line with art.13 of the Directive.

(f) Restrictions on onward transfers—other transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with art.26(1) of the Directive.

Examples of additional principles to be applied to specific types of processing are: **8–13**

(a) Sensitive data—where "sensitive" categories of data are involved (those listed in art.8 of the Directive22), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

(b) Direct marketing—where data are transferred for the purposes of direct marketing, the data subject should be able to "opt-out" from having his/her data used for such purposes at any stage.

(c) Automated individual decision—where the purpose of the transfer is the taking of an automated decision in the sense of art.15 of the Directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

Procedural and enforcement mechanisms

In Europe, there is broad agreement that data protection principles should be embodied in law. There is also broad agreement that a system of "external supervision" in the form of an independent authority is a necessary feature of a data protection compliance system. Elsewhere in the world, however, these features are not always present. **8–14**

To provide a basis for the assessment of the adequacy of the protection provided, it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries.

The objectives of a data protection system are essentially threefold:

(a) to deliver a good level of compliance with the rules. (No system can guarantee 100 per cent compliance, but some are better than others.) A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important part in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials;

(b) to provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his/her rights rapidly

160

(a) The contract should set out in detail the purposes, means and conditions under which the transferred data are to be processed, and the way in which the basic Data Protection Principles are to be implemented. Greater legal security is provided by contracts which limit the ability of the recipient of the data to process the data autonomously on his own behalf. The contract should therefore be used, to the extent possible, as a means by which the entity transferring the data retains decision-making control over the processing carried out in the third country.

(b) Where the recipient has some autonomy regarding the processing of the transferred data, the situation is not straightforward, and a single contract between the parties to the transfer may not always be a sufficient basis for the exercise of rights by individual data subjects. A mechanism may be needed through which the transferring party in the Community remains liable for any damage that may result from the processing carried out in the third country.

(c) Onward transfers to bodies or organisations not bound by the contract should be specifically excluded by the contract, unless it is possible to bind such third parties contractually to respect the same Data Protection Principles.

(d) Confidence that Data Protection Principles are respected after data are transferred would be boosted if data protection compliance by the recipient of the transfer were subject to external verification by, for example, a specialist auditing firm or standards/certification body.

(e) In the event of a problem experienced by a data subject, resulting perhaps from a breach of the data protection provisions guaranteed in the contract, there is a general problem of ensuring that a data subject complaint is properly investigated. EU Member State supervisory authorities will have practical difficulties in carrying out such an investigation.

(f) Contractual solutions are probably best suited to large international networks (credit cards, airline reservations) characterised by large quantities of repetitive data transfers of a similar nature, and by a relatively small number of large operators in industries already subject to significant public scrutiny and regulation. Intra-company data transfers between different branches of the same company group is another area in which there is considerable potential for the use of contracts.

(g) Countries where the powers of state authorities to access information go beyond those permitted by internationally accepted standards of human rights protection will not be safe destinations for transfers based on contractual clauses.

In the UK there is no legal barrier to a data controller making its own assessment of the adequacy of protection in the receiving country and this is acknowledge by the Commissioner in his Guide. If the controller proceeds in this way he does not need to make any submission to the Commissioner. The Guide advises that the controller should look at, in particular:

> "the extent to which the country has adopted data protection standards in its law; whether there is a way to make sure the standards are achieved in practice; (for

example, whether there are any enforceable codes or conduct or other rules); and whether there is an effective procedure for individuals to enforce their rights or get compensation if things go wrong."

The Guide provides a number of examples where a decision on adequacy may be made without a detailed analysis, for example the transfer of academic biographies of staff by a university or the transfer of information on telephone lists used by a global company. Data controllers who wish to rely on their own view that a country provides an adequate standard of protection will have to be able to demonstrate a rational decision-making process to show an assessment of adequacy.

COMMUNITY FINDINGS—STATES

8–18 At the time of writing, the European Commission has issued decisions recognising Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey and Switzerland[27] as providing adequate protection for personal data on the basis that those countries have generally applicable data protection law which follows the same approach as the Directive; although with respect to Canada this is not a finding for the jurisdiction as the Canadian Act, the Canadian Personal Information Protection and Electronic Documents Act, which came fully into force on January 1, 2004, do not cover personal data held by public bodies or by private organisations and used for non-commercial purposes. Accordingly where the data transfer is to a public body or to a private body for a non-commercial purpose, adequacy will have to be achieved by some other mechanism. There are also data protection laws in a number of States which should be taken into consideration. The Commission also made an adequacy decision with respect to Hungary in 2000, but Hungary has since joined the EU.

SAFE HARBOR

8–19 The US approach to the protection of personal privacy is different from the EU one. The US has a number of statutory protections but these are piecemeal and specific to sectors or particular problems, for example the Children's Online Privacy Protection Act 1998 (COPPA). Otherwise regulation is based on self-regulatory mechanisms and consumer action. This is very different from the EU approach of universally applicable law. The US Administration was concerned that personal data would stop flowing to the US after implementation of the Directive and accordingly the Safe Harbor Agreement was negotiated. The Safe Harbor Agreement is only one possible mechanism to allow data export to the US; reliance can be placed on any of the derogations, such as consent, or a contractual solution adopted. The Safe Harbor agreement has not been

[27] For a full up to date list of Adequacy decisions see *http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.*

universally popular. On the European side the Parliament expressed reservations about it as did the Article 29 Working Party. Nevertheless it is a significant initiative.

The details of the Safe Harbor Agreement are found in the Commission Decision of July 27, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce.[28] The papers consist of:

- the Decision itself;
- the Privacy Principles;
- the Frequently Asked Questions;
- a list of the US Statutory Bodies recognised by the EU as being able to deal with complaints and offer redress;
- correspondence from those authorities (the Federal Trade Commission (FTC) and the US Department of Transportation (USDoT)) to the Commission;
- a memorandum outlining the authority of the FTC; and
- a statement of the US law on damages for breach of privacy and explicit authorisations in US law.

The materials can be found on the EU website or the US Department of Commerce website, *www.export.gov/safeharbor*,[29] or *www.ita.doc.gov*[30] where a list of those companies which have decided to adopt the Safe Harbor Principles can also be found. The material recital in the Commission decision is (5) which reads:

> "The adequate level of protection for the transfer of data from the Community to the United States recognized by this decision, should be attained if organizations comply with the Safe Harbor Privacy Principles for the protection of personal data transferred from a Member State to the United States (hereinafter 'the Principles') and the Frequently Asked Questions (hereinafter 'the FAQs') providing guidance for the implementation of the Principles issued by the Government of the United States on 21.07.2000. Furthermore the organizations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive trade acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs."

This encapsulates the requirements of the Safe Harbor.

Overview

8–20 Participation in Safe Harbor is voluntary. It is only open to organisations which are subject to either s.5 of the Federal Trade Commission Act (FTCA) or the authority of the US Department of Transportation under Title 49, United States

[28] Decision 520/2000/EC.
[29] Accessed September 16, 2012.
[30] Accessed September 16, 2012.

163

Code, Section 41712. Section 5 of the FTCA does not apply to banks, savings and loans and credit unions, telecommunications and interstate transportation common carriers, air carriers and packers and stockyard operators. Most of these are therefore excluded from Safe Harbor unless covered by the Department of Transportation. This covers the travel industry and airlines. In order to join the Safe Harbor a US organisation must do one of three things: develop its own self-regulatory privacy policy which complies with the Principles[31]; participate in an industry self-regulatory programme which meets the Principles, for example the TRUSTe or BBBOnline programmes; or comply with sector-specific regulations that meet the Principles. The organisation must then certify to the Department of Commerce (or its designee) that it is operating in compliance with the Principles. The certification must include specific information including a statement that the organisation has a privacy policy, which is available to the public, and which complies with the Principles. The notification lasts 12 months and the organisation must make an annual return to the Department confirming its continued compliance. This is called a verification and may be based upon a self-assessment or a compliance review by an outside body. Participants have to have effective enforcement and dispute resolution mechanisms which can be delivered either by a private sector organisation such as BBBOnline or by committing to cooperate with EU data protection authorities. The co-operation option must be chosen where the data controller in the EU plans to transfer personal data about employees in the EU. Where the cooperation option is chosen the company works with a panel drawn from the supervisory authorities in the EU. Failure to comply with the self-regulatory standards must be actionable under s.5 as an unfair or deceptive act or some other statutory mechanism. The organisation only has to apply the standards to data which it receives by way of transfer from the EEA after the adoption of the Safe Harbor. The standards are not applicable to manual information which falls outside the Directive but can be applied if the organisation chooses. If an organisation wishes to include human resources data in the Safe Harbor it must indicate that fact specifically in its certification. An organisation can decide to leave Safe Harbor but the personal data which it received from the EU during its membership must continue to be treated in accordance with the Principles.

Safe Harbor—the Privacy Principles

The seven Privacy Principles are issued by the US Department of Commerce under its statutory duty to foster, promote and develop international commerce. In view of their importance they are set out in full below: **8–21**

"• Notice
An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any enquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is

[31] In this context "Principles" means the Safe Harbor Privacy Principles.

practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

- Choice
  An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear, conspicuous, readily available and affordable mechanisms to exercise choice.
  For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of an opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.
- Onward transfer
  Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing. If the entity in Safe Harbor discloses other than to an agent the onward transfers may only be made in accordance with the Notice and Choice Principles. That is to say that onward transfers are only permitted where the data subjects have been notified about the types of third parties to whom the data are disclosed and offered the possibility to opt out of such third party disclosures. It is therefore only possible to rely on Safe Harbor for onward transfers in these circumstances where data subjects are notified and offered opt-out choices.
- Security
  Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorised access, disclosure, alteration and destruction.
- Data integrity
  Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organisation may not process personal information in a way that is incompatible with the purpose for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current.
- Access
  Individuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information

165

Comment

The Privac
particular t
on automa
governing
Otherwise

The Freq

There are
;secondary
authorities
with Safe
processor
informatio
publicly a
the practic

US regul

The basis
privacy p
Failure to
So the po
which ex
(FTC) an
the US.
which an
also shov

where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

- Enforcement
Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include, (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations."

Comment

The Privacy Principles do not meet all the requirements of the Directive. In particular the individual rights to object to some kinds of processing and the ban on automated decisions are absent. Moreover there are no specific rules governing telecommunications as there are in Europe under Directive 2002/58. Otherwise the Principles are close to the requirements of the Directive.

The Frequently Asked Questions (FAQs)

There are 15 FAQs. The FAQs relate to: sensitive data; journalistic exemptions-;secondary liability; investment banking and audits; the role of data protection authorities; self-certification under the Safe Harbor; verification of compliance with Safe Harbor; the access principle; personal data used for human resources; processor contracts; dispute resolution and enforcement; timing of opt outs; travel information; pharmaceutical and medical products; and public record and publicly available information. The FAQs amplify the Principles and deal with the practical points relating to the working of the Safe Harbor. **8–22**

US regulatory bodies and correspondence from them

The basis of Safe Harbor is that the organisation "signs up" to a publicly stated privacy policy that incorporates the standards set out in Principles and the FAQs. Failure to comply with that privacy policy can be the subject of regulatory action. So the policy becomes enforceable by an independent regulator. The two bodies which exercise relevant regulatory powers are the Federal Trade Commission (FTC) and the US Department of Transportation. Enforcement will take place in the US. The Department of Commerce maintains the public list of subscribers which anyone wishing to export personal data to the US may consult. The list also shows the enforcement body for the subscriber so it can be used by anyone **8–23**

wanting to make a complaint. Enforcement action by the regulator may result in the subscriber being struck off the list and losing Safe Harbor status. If a company loses Safe Harbor status that will be made clear in the list. The FTC has undertaken, in the correspondence with the EU, to give priority to referrals of non-compliance with Safe Harbor received from privacy programmes or EU data protection authorities.

Financial services

8–24 As such services are not subject to s.5 of the Federal Trade Commission Act they are not able to take advantage of the Safe Harbor. Discussions are continuing between the EU and the US over bringing financial services into Safe Harbor but have not yet reached fruition at the time of writing.

Can data processers join the Safe Harbor?

8–25 The Department of Commerce (DoC) has accepted Safe Harbor self-certifications from a number of organisations in respect of their activities as data processors (see, for example, the Hewlett-Packard self-certification). However the application of the Safe Harbor Framework to a data processor is not wholly straightforward. The position of processors in Safe Harbor is explicitly covered in the FAQs under the title "Article 17 Contracts". The question and answer are set out:

> "When data is transferred from the EU to the United States only for processing purposes, will a contract be required, regardless of participation by the processor in the safe harbor? Yes. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU. The purpose of the contract is to protect the interests of the data controller, i.e. the person or body who determines the purposes and means of processing, who retains full responsibility for the data vis-à-vis the individual(s) concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure. A U.S. organization participating in the safe harbor and receiving personal information from the EU merely for processing thus does not have to apply the Principles to this information, because the controller in the EU remains responsible for it vis-à-vis the individual in accordance with the relevant EU provisions (which may be more stringent than the equivalent Safe Harbor Principles). Because adequate protection is provided by safe harbor participants, contracts with safe harbor participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the Member States) as would be required for contracts with recipients not participating in the safe harbor or otherwise not providing adequate protection".

It appears from this FAQ therefore that, under US law, a US entity which is enrolled in Safe Harbor is not required to comply with the Safe Harbor Privacy Principles where it is acting as a mere processor for an EU controller. However under Commission Decision 2000/520/EC art.2, an EU data controller may only transfer data to the US where the recipient U.S. organisation has "unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs" in respect of "each transfer of data". On the

167

face of it this would suggest that the entity must comply with the Principles even if it is a processor. It should be noted that the obligation is to comply with the Principles implemented in accordance with the FAQs, not the Principles simpliciter. The view may therefore be taken that the response to the FAQ quoted above alters the usual position and a processor who applies the line taken in the FAQ will be meeting the Principles implemented in accordance with the FAQs. It has to be said that this is not a wholly satisfactory position. While compliance with some of the Principles, on the face of it, lies in the gift of the controller rather than the processor, such as Notice and Choice, at least some of the obligations in the Principles can, and should, be complied with by the processor such as security principles. Equally a processor could enter into a contract with the controller under which the controller could deal with those aspects of the Principles which are clearly within his gift, such as notice and choice to data subjects. The position is less certain re the access Principle. A controller could authorise the processor to respond to subject access requests as its agent subject to appropriate limits however it might be preferable for the parties to agree that, if an access request is received by the processor, the controller will deal with it. The effect of the contract would be to ensure that the Safe Harbor Principles are met even if not directly by the processor.

Safe Harbor and the Cloud

The Working Party have stated that " ... sole certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment."[32] The Working Party encourages customers to obtain evidence that the Safe Harbor principles are being complied with; although no practical guidance is provided about what additional information beyond a certification should or must be sought. Notwithstanding these reservations national data protection authorities have not suspended data flows to a Safe Harbor-certified organisation and notifed the Commission accordingly. They are entitled to do so if there is substantial risk that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continued transfer would cause an imminent risk of grave harm to data subjects; and the competent authority has made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond. It therefore seems reasonsonble to conclude that a transfer to a Safe Harbor certified organisation is an acceptable way to achieve adequcy which respect to that transfer and any onwards transfer that falls withth the Safe Harbor framework; although the cloud customer must of course also compy with the other requirements of Directive 95/46/EC in relation to the transfer and subseqent procesing. **8–26**

[32] WP Cloud Opinion, p.17.

168

CONTRACTUAL CLAUSES APPROVED BY THE COMMISSION

8–27 Individual contracts or sets of contractual clauses do not, of course, provide an adequate level of protection for an entire country. Thus contractual clauses are a way of complying with an exemption to the Eighth Principle rather than complying with the Principle itself.

The provisions in the Directive have not been translated directly into the 1998 Act. Instead the exemptions set out in Sch.4 provide that the Eighth Principle does not apply where:

> "The transfer is made on terms which are of the kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects."[33]

Thus, there is no specific reference to contractual terms or clauses.

There is no barrier to individual data controllers agreeing contracts with third parties for the export of personal data on terms negotiated between the parties. In many EU countries such contracts have to be submitted to the national supervisory authority for approval. The United Kingdom and Ireland are exceptional in that the regulators have not required the submission of contracts. Where contracts have to be submitted the national authority will usually review the terms to ensure that certain standards are met and if it considers the contract to be deficient may require amendments. It can take several months for contracts to be approved. Standard form clauses are intended to shorten the process as the national regulatory authorities have to accept contracts drawn up in accordance with the standard.

Three sets of clauses are currently approved by the European Commission for use; two sets of controller to controller clauses and one set of controller to processor clauses. The standard form contracts are very similar even though the legal relationships between the parties are very different. The contracts have been approved under art.26.2. They are not mandatory (at least not in theory) —controllers may still use their own contracts—but where the standard forms are used, in most cases, the national regulators have to accept them as producing adequate protection.

Controller to controller contract

8–28 On June 15, 2001 the Commission approved a standard set of contractual clauses to cover the situation where a data controller in the EU sends personal data to a controller outside the EEA to a jurisdiction which does not offer adequate protection for the personal data.[34] The Decision took effect in September 2001. The UK Information Commissioner authorised transfers made using the model clauses under para.9 of Sch.4 on December 21, 2001. The standard contract has been criticised as it imposes onerous obligations, particularly on the recipient. If a data controller uses the clauses then the contract should be accepted by data

[33] Sch.4 para.8.

[34] Commission Decision 2001/497/EC of June 15, 2001 on standard contractual clauses for the transfer of personal data to third countries under Dir.95/46.

169

protection authorities in all the Member States as providing adequate protection. The contract is intended to take effect under the law of the exporting Member State so the contract has to be altered at least so as to accommodate any legal requirements to comply with contract law in the Member State.

The standard clauses offer a number of options to reach a standard of adequacy. The contract can incorporate standards equivalent to the data protection law of the sending country; or (if the importer is US based and does not already subscribe to Safe Harbor) the Safe Harbor Principles; or the Principles set out in the standard form contract.[35] The data exporter agrees that the transfer complies with the national law and is liable for compliance with the national law up until the export[36] and remains liable for continued compliance with the Principles jointly with the importer.[37] The individual data subjects are entitled to copies of the contract and to have their queries answered by both parties.[38] They must be told of any sensitive data export[39] and be able to enforce rights under the contract.[40] In England and Wales this can now be done by virtue of the Contracts (Rights of Third Parties) Act 1999. The importer agrees to abide by rulings of the national supervisory authority in the exporting jurisdiction and to submit to audit by the exporter.[41]

The contract has appendices in which the parties set out the categories of data subjects about whom data are being transferred, the purpose of the transfer, the categories of personal data being exported, the recipients of the data, the storage limit, i.e. the length of time for which the data will be held, and where sensitive data are involved, the types of sensitive data.

The Commission has published a set of FAQs on the standard clauses which is also available on the Commission website and which covers: **8–29**

- whether the clauses are compulsory;
- whether companies can rely on contracts approved at national level;
- whether Member States can block or suspend transfers where the standard clauses are used;
- whether the clauses can be used as part of a wider contract;
- the relation between the Principles and any derogations to those imposed by the importer's national law;
- the burden of joint and several liability;
- the relation with the "safe harbor"; and
- whether those who are not members of the "safe harbor" can use the "safe harbor" aspect of the standard.

The adoption of the clauses was preceded by correspondence with the US interests represented by both the US Departments of Treasury and Commerce (April 2001) and an Opinion prepared by the Article 29 Working Party on January

[35] cl.5b.
[36] cl.4a.
[37] cl.6.2.
[38] cll.4c and 5c.
[39] cl.4b.
[40] cl.6.1.
[41] cl.5c and d.

170

26, 2001. The documents, which are available on the Commission website, show the divergence of positions between the Americans and Europeans over the privacy debate.

Contracts (Rights of Third Parties) Act 1999—England & Wales

8–30 Under the law of England and Wales, a person who is not a party to a contract may enforce a term of a contract if either the contract expressly provides that he may, or the term purports to confer a benefit on him, unless it is clear from the contract that this was not intended by the parties.[42] The third party has to be expressly identified in the contract, either by name or as a member of a class or answering a particular description.[43] This can easily be achieved in overseas transfer contracts by a description of the beneficiaries as employees or some other category. Such a clause will cover future members of the class as well as those in the class at the time the contract is entered into.[44]

The third party's rights apply under the contract so any exclusions or limitations in the contract will apply to him and he will only be able to exercise the remedies that apply under the contract.

Once a third party has become the beneficiary of a contract term his position is protected. The main parties cannot alter the term, or rescind the contract altogether, without the third party's agreement if it would disadvantage the third party because the third party has relied on the term.[45] Otherwise parties could enter into contracts which confer benefits on third parties to allow them to achieve some end, for example make an overseas transfer, and then rescind the contract once the transfer had been made, leaving the third party with no redress. A court, however, can dispense with the agreement of the third party in some cases.

The implementation of the third party rights has made contractual solutions an option for UK data exporters, who wish to contact under the laws of England and Wales. Scots law has always provided for third party rights.

Amendment of controller to controller clauses

8–31 The first set of controller to controller Commission approved contracts were not popular with business. The US Department of Commerce and the Department of the Treasury indicated their disagreement with aspects of them, as well as US business organisations. A more business friendly proposed standard contract was prepared by an alliance of business organisation including the International Chamber of Commerce and was accepted by a decision amending the original Commission decision on December 27, 2004.[46] These were authorised by ICO on May 27, 2004. There are now two sets of model controller to controller clauses, Set I and Set II. Data controllers may choose either set but may not amend the

[42] Contracts (Rights of Third Parties) Act 1999 s.1.
[43] 1999 Act s.1(3).
[44] 1999 Act s.1(3).
[45] Contracts (Rights of Third Parties) Act 1999 s.2.
[46] Commission Decision of December 27, 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard clauses for the transfer of personal data to third countries (2004/915/EC).

171

clauses or the sets. Each set is designed to achieve a balance of protection but does so by the use of different mechanisms. In each case the national supervisory authority in the exporting Member State may prohibit the data flows where certain conditions are satisfied. Set II does not include the joint and several liability clauses as between the importer and the exporter, the parties are liable for their own breach. However the exporter has an obligation of due diligence to determine that the data importer is able to satisfy its obligations under the contract and must agree to submit to data audits on reasonable request of the exporter. Where Set II has been adopted the rights of individuals to enforce for breach of the required standards is directed in the first instance to the exporter and only arises against the importer where exporter has refused to enforce the contract. Set II allows for rather more flexibility over agreements between the parties as to which one should deal with subject access requests. Under Set II rights of termination for breach of the contract are explicitly covered.

Controller to processer contract

On December 27, 2001 the Commission approved a set of model clauses to be used where a data controller in the EU sends personal data to a processor outside the EEA in a jurisdiction which does not offer adequate protection for the personal data.[47] The decision took effect on April 3, 2002. The UK Commissioner issued an authorisation in respect of contracts made using this model. The standard contract is designed to give enforceable rights to data subjects. This involves the exporter "agreeing" with the importer that his actions comply with the requirements of the Directive[48] although this seems unnecessarily complicated as the data subject would have a remedy under national law in any event if the exporter had failed in his compliance. The importer agrees to an audit of his processing if required,[49] to only process on the instructions of the processor and to implement the technical security measures which are set out in the Appendix to the contract.[50] The data has to be described in a similar way to the controller to controller contract.[51] Where data subjects suffer damage in the first instance they must seek any remedy against the exporter of the data[52]; however, if the exporter has disappeared or become insolvent the importer agrees that a claim may be made against him.[53] The contract provides for the return or destruction of the data at the termination of the contract.[54]

8–32

[47] Commission Decision of December 27, 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Dir.95/46/EC.
[48] cl.4.
[49] cl.5f.
[50] cl.5a, b, c.
[51] Appendix 1.
[52] cl.6.1.
[53] cl.6.2.
[54] cl.11.

172

Amendment of controller to processer clauses

8–33 New model clauses were approved in February 2010 for data controller to data processor transfers and came into effect from May 15, 2010.[55] These replace the 2001 clauses for new contracts rather than providing a second option, as with the controller to controller transfers. The main difference between the new clauses and the previous version is that the new clauses take account of the expansion of processing activities and deal with the situation where there is further outsourcing of processing to sub-processors. A definition of sub-processors has been added. This extends not just to someone acting as a sub-processor to the main processor (data importer) but to sub-processors engaged by sub-processors—so the requirements flow all the way down the chain. A data importer must not subcontract without the prior written consent of the data exporter and then only by way of a written agreement imposing the same obligations on the sub-processor as the model clauses impose on the data importer (the model clauses suggest that this could be satisfied by the sub-processors co-signing the contract between the data exporter and the data importer). The data importer remains fully liable for the activities of its sub-processors. The data importer is required to send a copy of any sub-processing contract to the data exporter. The data exporter is required to keep a list of the sub-processing agreements which have been concluded and update this at least once a year. This should be available to the data exporter's supervisory authority, in the UK the Information Commissioner.

Contractual clauses for international transfers and the cloud

8–34 "Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space".[56]

Cloud is not new but the pace of adoption and the range of cloud services have increased dramatically in recent years. As the Working Party acknowledge cloud based services can bring economic benefits in that on-demand services can be set up, scaled and accessed quickly and easily. However these flexible new computing solutions must operate within the existing data protection framework, including the rules on international transfers. There has been a wide range of debate about whether the existing legal structures are fit for the modern cloud.

8–35 In most cloud arrangements, but not all, the customer will be the data controller and the cloud provider a data processer; as in traditional outsourced relationships. This means that use of the controller to processer clauses may provide a way of achieving compliance if the cloud provider has part of its operations in a third country. However in some cases the cloud provider may undertake activities akin to those of a data controller and in those situations the data controller to data controller clauses or some other mechanism may be more appropriate. Customers will want to assess the status of the parties carefully

[55] Commission Decision of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593).

[56] Working Party Opinion 05/2012 on Cloud Computing 01037/12/EN WP 196 July 2012.

before deciding which adequacy mechanism is the most appropriate. Customers should undertake that assessment with care. Modern cloud providers often offer standard packaged services which cannot be varied or made bespoke to customer requirements. However, standardisation should not be confused with a lack of control. Customers can choose to use a service or not. As the Working Party states:

> "...clients of cloud computing services may not have room for manoeuvre in negotiating the contractual terms of use of the cloud services as standardised offers are a feature of many cloud computing services. Nevertheless, it is ultimately the client who decides on the allocation of part or the totality of processing operations to cloud services".[57]

On the other hand some services may mean that an element of control is lost over how data are processed and customers need to consider the status of the parties against that backdrop.

8–36 Cloud services often involve a number of contracted parties that act as data processers. Sometimes these third parties are within the cloud provider's group of companies, sometimes not. The Working Party point out that although sub-processing is permitted under the controller to processer clauses, this must be with the prior written consent of the controller.[58] Many cloud providers require this consent to be provided upfront as part of their terms and conditions of service, pointing out that it would be unreasonable to expect them to collect consent on a case by case basis from every customer given the complexity and rapidly changing nature of the cloud environment. The Working Party has acknowledged that this is acceptable practice provided the processer has a right to terminate if unhappy with any change.[59] This latter requirement has proved controversial and such a right remains by no means uniform in many cloud contracts.

8–37 In addition to sub-processing issues, use of MCCs for cloud services can give rise to a range of other practical issues including provision of audit rights to customers (which may not be practical for security and scalability reasons), detailing the location or locations data are processed (which again is not always practical for security reasons) and deciding on the right contract structure where often the group structures of both the customer and cloud provider are complex.

BINDING CORPORATE RULES

8–38 Although the Directive does not provide any mechanism for the Commission to approve group wide codes of conduct as an acceptable mechanism to deliver adequacy, such codes have been increasingly used.[60] They offer global businesses, which may be subject to a large number of different privacy laws, a

---

[57] Ref.52, p.8.
[58] Ref.52, p.10.
[59] Ref.52, p.10.
[60] The code developed by Shell for its global business was the starting point for the ICX draft code which was considered by the IPSE initiative under the work carried out by CEN. See *www.cenorm.be* [Accessed September 16, 2012] for a Report on the IPSE work.

174

method of standardising compliance levels in the business. There was some interest in the possibility of developing a standard form code which could be adopted by business and used as a tool to enable the transfer of personal data intra-group.[61] It gradually became clear that one code would not be able to deal with the vast range of data processing activities but the way forward would be for global companies to develop individual "codes" which meet the necessary standards. These codes are called Binding Corporate Rules. In outline a company works with a national supervisory authority to adopt a binding internal code which the supervisory authority then approves under the national implementing provisions of art.26(2). Article 26(2) allows Member States to authorise transfers to countries which do not ensure an adequate level of protection where the controller,

> " ... adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals as regards the exercise of the corresponding rights".

The scheme put forward for approval must therefore be able to deliver guarantees of compliance and rights of redress for non-compliance. The relevant national supervisory authority is responsible for liaising with the other relevant data protection authorities in other jurisdictions to obtain the agreement of all.

Originally BCRs could only be used for controllers (i.e. covering "your own data"). More recently the concept has been extended to cover data processors. (i.e covering "third party data").[62] WP 195 sets out the main elements that the Working Party would like to see included in processor BCRs; taking existing criteria for the approval of a BCR and translating what that might look like in a processor BCR. BCRs for processors do not stand alone and must be linked to an Service Level Agreement with the data controller.

Article 29 Working Documents on Binding Corporate Rules[63] (BCRs)

8–39 The field of BCRs has become increasingly complex and it is difficult to summarise the myriad of Working Party guidance in this short chapter. Those considering BCRs are advised to review the full set of Working Party papers[64]; in particular WP 74, WP 108 and WP 155.

8–40 The Working Documents makes it clear that BCRs should not be regarded as having superseded contractual solutions; such solutions are being used in increasingly sophisticated ways, for example by having standard clauses with many parties to the contract. It is emphasised that BCRs may be used with contractual solutions, for example the initial transfer may be made under BCRs and further onward transfers to other recipients than the data importer under separate contractual arrangements. Such contractual solutions can allow for further transfers where the data subjects have given unambiguous consent (where

[61] See the work carried out by the Initiative for Privacy Standardisation in Europe Report at the CEN website *www.cen.be* [Accessed September 16, 2012].
[62] WP 195.
[63] WP 195.
[64] WP74, WP108, WP133, WP153, WP154, WP155 and WP195.

175

sensitive data are concerned) or in other cases been given the opportunity to object. The various documents which set out the standards which must be reached to produce BCRs use slightly different terminology and sequence. In this section we examine the topic by reviewing the substantive content required and then the procedure for authorisation.

The application follows a two stage process. Before embarking on the BCR process proper organisations need to make an initial application to obtain the co-operation of the supervisory authority with which the organisation wishes to work and ascertain that it has the jurisdiction to approve BCRs. As WP 108 makes clear the BCR process is not mandated by the Directive and the participation of supervisory authorities is therefore not required under EU law. WP 108 states that: "The participation of data protection authorities in the approval of binding corporate rules is entirely voluntary". While this is accurate in general terms the UK Commissioner has set out the terms and process on which his office will work with organisations in this area. If he failed to honour those public statements without some good reason an aggrieved applicant might have public law remedies. **8–41**

Jurisdiction

A corporate group which wishes to pursue the BCR approach must select the lead data protection supervisory authority using the criteria set out in the guidance. The initial application is made to the selected lead data protection supervisory authority showing the nature and general structure of the processing activities in the EEA/EU with particular attention to: **8–42**

- the place where decisions are made;
- the location and nature of affiliates in the EU;
- the number of employees or others concerned;
- the means and purpose of the processing;
- all the places from which the transfers to third countries take place; and
- the third countries to which data are transferred.

The recipient authority will forward the information to all of the supervisory authorities which have a supervisory role for the processing described with a statement as to whether it is prepared to be the lead authority. The authorities will agree among themselves within a period of approximately two weeks as to whether the choice of the lead is appropriate. Once the lead authority has been agreed that authority will work with the applicant to agree the substantive provisions and prepare the deliverables for submission. The lead authority is responsible for circulation of the BCR to other DPAs under the mutual recognition or co-operation procedures. Under the original co-operation process all DPAs have the opportunity to make comments on the draft BCR; which can be time consuming. Under mutual recognition once the lead authority considers that the BCR meets the requirements the draft BCR is circulated to other mutual recognition countries. The DPAs under mutual recognition accept this opinion as sufficient basis for providing their own national permit or authorisation. Over 20 countries are currently signed up to the mutual recognition procedure.

176

Substantive Provisions

Data Protection Lead

8–43 The corporate must identify a member of its corporate structure within the EU which will be the lead for the purposes of data protection compliance. Either this will be the corporate headquarters or the member of the group which has delegated data protection responsibilities for the group. This entity works with the supervisory authority for the Member State in which it is situated to achieve the BCR approval. WP108 sets out a set of criteria for choosing the correct entity and jurisdiction if the parent or operational headquarters is situated outside the EU. The chosen corporate entity must be appointed by the parent with data protection responsibilities for the corporate group to ensure that the chosen corporate can impose data protection compliance standards on members of the group outside the non-EEA, have authority to work with the chosen data protection authority and takes responsibility for the payment of compensation for damages resulting from a breach of the BCRs by any liable member of the corporate group.

Description of processing and data flows

8–44 The documents submitted for BCR approval (and there may be a suite of such documents—there is no requirement that applicants submit one compendious document) must identify the nature of the data, for example the rules may only relate to one kind of data such as human resource data, the purposes of the transfer, and the extent of the inter-group transfers. The description of the transfers must cover those within the EEA and those outside the EEA and any onward transfers to third parties from those outside the EEA. The level of detail may mirror a detailed notification.

Data protection safeguards

8–45 The data protection compliance standards adopted in respect to the data must be set out. These must comply with the law of the Member State where the responsible corporate is situated and be consistent with the Directive. These rules are to be applicable to all of the defined personal data transferred through the defined corporate group. It should be noted that there may be different standards of enforceability (see later). The OIC notes that this should be more than a restatement of the DPA and contain some "added value" for example practical guidance to staff. The Rules must address:

- transparency and fairness to the data subject;
- purpose limitation;
- ensuring data quality;
- security;
- individual rights of access, rectification and objection to processing; and
- restrictions on onward transfer out of the multinational company covered by the rules.

177

Legally binding measures

The crux of the mechanism is that the rules must be "binding" both within the corporate and for the benefit of individuals. There is a certain inevitable elasticity to the term "binding". Inevitable because to quote WP74 BCRs are intended to be available to a range of organisations "on the basis of different legal and cultural backgrounds and different business philosophies and practices". Although the term "binding" appears at first sight to be synonymous with "legally enforceable" a closer reading of the material suggests that BCRs may be acceptable if they are enforced in practice even if the organisation is not been able to offer a mechanism which is entirely legally enforceable.

Binding within the organisation

The rules may be made binding by contracts within the group or as corporate codes adopted by a group. WP 74 notes that:

Under international corporate law affiliates may be able to enforce codes of conduct against each other based on claims of quasi-contractual breach, misrepresentation or negligence.

The effect may also be achieved by unilateral undertakings given by the parent company and which are binding on members of the group; by the adoption of codes which are capable of having a regulatory effect within an existing legal framework or by incorporating the rules into the general business principles of the organisation backed by appropriate policies, audits and sanctions. This last possibility appears in WP 108 but not in the ICO Guidelines. This may be because such rules would not be enforceable under UK law.

Binding on employees

Employees must be bound to take account of the rules and this may be achieved by including requirements in contracts together with the provision of appropriate training backed up with sanctions for non-compliance.

Binding on sub-contractors

This may be achieved by the incorporation of suitable clauses into contracts.

Binding for the benefit of individuals

It is only mandatory that those data subjects whose personal data emanates from the EU have the right to enforce the BCRs, although the extension of the benefit to others will be welcomed by supervisory authorities. This entails both that individuals are able to pursue a judicial remedy and that the data protection lead corporate is subject to and accepts the supervision of the data protection supervisory authority. Individuals must be able to take lodge their complaints with the member of the group at the origin of the transfer (within the EU) or the group member which is the data protection lead. The lead corporate must demonstrate that it has sufficient financial resource to deal with any claim. The rules must become binding for the benefit of the data subjects by some legal

178

mechanism such as by acquiring third party rights under inter-group contracts. WP 74 notes that in some jurisdictions unilateral declarations by corporates may be sufficient to be the origin of third party rights but in other legal systems this is not the case. The Guidance from the UK Commissioner focuses on the practical steps which must be open to complainants but does not explore the enforceability of the rules by data subjects. WP 74 notes however that all the data subjects will have rights under the data protection laws of the country where personal data relating to them was processed. The remedies available must be equivalent to those mandated by the Directive.

Compliance audit & training, and complaints

8–46 The WP attaches significance to the verification of compliance. The rules must provide for audit by either internal or external auditors or a combination. The supervisory authority is entitled to call for the audit programme to be provided to it. The supervisory authorities will be expected to undertake to only have regard to the material relating to the data protection audit and not to other matters of corporate governance. It is important to include a description of the audit system and a commitment to share audit results with the board of the parent. There should be a commitment to provide training on the requirements of the BCR as well as a detailed explanation of the training programme. A mechanism for complaints handling should also be detailed.

Mechanism for recording and reporting change

It is recognised in WP 74 that "... corporate groups are mutating entities whose members and practices may change from time to time..." and thus the deliverables must include processes to deal with such change. These must ensure that:

- no transfer is made to a new member of the group until the new member is bound by the rules and able to deliver compliance with them;
- an updated list of the group members, the rules and any update to the rules is maintained and made available to the supervisory authority on request; and
- updates and changes are notified to the data protection authorities annually

Procedures and deliverables

8–47 The lead corporate works with the supervisory authority to ensure that its submission reaches the proper standard. It must submit:

- a background paper setting out how the required substantive elements of the BCR structure have been met;
- the set of materials which comprise the rules which are to be adopted by the group; and
- the contact details of a responsible person in the organisation.

179

This material, referred to in WP108 as a "consolidated draft", is distributed among the relevant supervisory authorities for comment. The period allowed for comment is usually one month. The lead authority will transmit the comments to the applicant and, where necessary there will be further work and discussion to deal with any unresolved problems. Once the lead authority considers that the material is satisfactory it will invite the applicant to send a final draft which can be circulated to all the relevant supervisory authorities for confirmation. The formal approval for the BCR will issue from the lead authority but the confirmation from the relevant supervisory authorities acts as authorisation for the transfer arrangements at each national level. Once approval is granted the Chairman of the Article 29 Working Party will notify all supervisory authorities.

COMMISSIONER'S GUIDANCE

Section 51(6) imposes the following relevant obligation on the Commissioner: **8–48**

> "The Commissioner shall arrange for the dissemination in such form and manner as he considers appropriate of:
>
> (a) any Community finding as defined by paragraph 15(2) of Part II of Schedule 1;
> (b) any decision of the European Commission, under the procedure provided for in Article 31(2) of the Data Protection Directive, which is made for the purposes of Article 26(3) or (4) of the Directive; and
> (c) such other information as it may appear to him to be expedient to give to data controllers in relation to any personal data about the protection of the rights and freedoms of data subjects in relation to the processing of personal data in countries and territories outside the European Economic Area."

The "Community findings" referred to in subs.(a) have been discussed in para.8–20, above. Subsection (b) refers to procedures set out in the Directive for approval of standard contractual clauses which have been discussed above.

Under the previous Commissioner, Elizabeth France, the approach to cross border transfers differed from that of some national supervisory authorities. It has been noted earlier that the UK Commissioner has not sought to approve transfers made under the derogations nor individual contracts made between controller and controller. The Guidance issued by the Commissioner also accepted that where a transfer was made from a controller to a processor it was regarded as sufficient to achieve compliance if the parties had entered into a contract which met the requirement of principle 7. When the guidance was re-issued by Richard Thomas in June 2006, there appears to have been some stepping back from this generous view. The current Guidance consists of the Guide to Data Protection plus material on the website issued in summer 2012 which consists of an overview and four specific topic guides. This suite of guidance replaces the earlier guidance on the eighth principle and international transfers. One of the topic guides covers outsourcing.

The outsourcing guide covers international outsourcing to data processors located in a third country. It emphasises the requirement to satisfy the eighth as well as the seventh principle. It rehearses the basic requirements of principle 7 **8–49**

180

and emphasises that, where processing of personal data is outsourced to a processor, the data controller remains responsible for compliance with the Principles. This includes the obligation on the controller to ensure that the processor provides appropriate security and is bound by a contract made or evidenced in writing. It suggests that an appropriate way of achieving compliance with both principles is the use of the model contract for processor or controller to processor transfers. However it recognises that this is not the only way to satisfy principle eight and other methods of establishing adequacy may be acceptable.

8–50 Interestingly, the Commissioner does not wholly close the door on the use of contracts which satisfy principle 7 although it is clear that the controller who wishes to use such a contract as the basis of the outsourcing transfer must also be able to show that they have satisfied all of the adequacy requirements. The relevant paragraph from the Outsourcing Guide states:

> "You do not necessarily need to use the model contract clauses when entering into an international outsourcing arrangement if you have found an alternative means of complying with, or using an exception to, the Eighth Principle. For example, ensuring compliance with the security requirements of the Seventh Principle will go some way towards satisfying the adequacy requirements of the Eighth Principle (given the continuing contractual relationship between you and your processor and your continuing liability for data protection compliance under the Act)."

In the Sending Personal Data Outside the EEA Guide itself it accepts that a transfer can be made to a processor in reliance on a combination of an adequacy assessment and an appropriate contract:

> "In some cases you might reasonably decide there is adequate protection without a detailed assessment. A common situation is where you transfer personal data to a processor acting on your instructions under contract. You are still legally responsible for making sure the data is processed in line with the principles. In particular, personal data can only be transferred if there is a contract requiring the processor to have appropriate security and act only on your instruction. So individuals' information should continue to be protected to the same standard as in the UK and they will have the same rights they can exercise in the UK. This is because you remain liable for ensuring that the processing complies with the data protection principles. When selecting a processor, you need to satisfy yourself that it is reliable and has appropriate security.
>
> However, the level of protection is unlikely to be adequate if:
>
> - the transfer is to a processor in an unstable country; and
> - the nature of the information means that it is at particular risk".

It also explains that data controllers can use their own contracts "to help ensure adequacy for a transfer or set of transfers" where the contract is used to "plug gaps". It notes that contracts can also be used where the data controller is not in a position to judge adequacy and advises that the contract should be comprehensive. It warns that if a data controller uses contract provisions which are different from the model clauses it risks a future challenge to the adequacy of the level of protection provided by the contract.

Fair processing and overseas transfers

The provision of information to a data subject about the implications of any cross-border transfer of their personal data is likely to be part of the provision of the "specified information" required by the fair processing code. 8–51

The first principle provides, inter alia, that data are not to be treated as being processed fairly unless the data subject is provided with certain information at the time that the data are gathered from him or, if the data are obtained by another route (presumably purchase or transfer from another data controller), either before the first processing or disclosure or as soon as practicable thereafter.

The information to be provided to the data subject is as follows:

(a) the identity of the data controller;
(b) the identity of any nominated representative;
(c) the purpose or purposes for which the data are intended to be processed; and
(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

The "any further information" requirement would appear to encompass providing the data subject with information about any non-obvious country to which his/her personal data may be transferred and the implications of such a transfer, although it is not clear or established as a matter of practice just how much information should be provided in order to make the processing fair; especially in the cloud context where data processing location may vary after the date on which data subject is notified. It is submitted that a general statement that that processing may take place outside the EEA (with safeguards) is sufficient; unless the particular risks mean that the data controller has assessed that normal safeguards do not sufficiently manage or mitigate risk to a level that the data subject is likely to find acceptable.

In cases where the consent condition of Sch.4 is being relied upon it is likely that the specified information requirements of the First Principle and the consent condition of Sch.4 will be dealt with in tandem so that data controllers develop specific written or spoken procedures which both convey information about any intended overseas transfer to the potential data subject and obtain his or her consent. This might be achieved, for example, by providing the data subject with a written notice in duplicate detailing the specified information and asking for the return of one copy signed to indicate consent.

EXEMPTIONS OR DEROGATIONS

Schedule 4 to the 1998 Act, following art.26(1) of the Directive, sets out a limited number of situations in which an exemption from the "adequacy" requirement for third country transfers may apply. The interpretative provisions in Pt 2 of Sch.1 indicate that the eighth principle simply does not apply to transfers covered by one or more of the criteria set out in Sch.4. 8–52

182

These exemptions, like most of the exemptions to general principles in the 1998 Act, are tightly drawn. Broadly speaking, they cover three situations—first, where the risks to the data subject are relatively small secondly, where other interests (public interests) override the data subject's rights, and thirdly where the transfer benefits the data subject.

There are many similarities between the exemptions set out in Sch.4 and the conditions for processing set out in Schs 2 and 3. In some cases, the provisions are identical.

The interpretative provisions[65] reserve the right of the Secretary of State to make orders directing that transfers prima facie falling within the list of exemptions may still be governed by the eighth principle.

The first of the exemptions in Sch.4 covers cases where the data subject gives his/her consent to the proposed transfer.

Article 26(1)(a) of the Directive refers to the data subject giving his/her unambiguous consent. The word "unambiguous" does not appear in the relevant provision in Sch.4 to the 1998 Act. Article 2(h) of the Directive, which contains the definition of consent, states that it must be freely given, specific and informed. The requirement that consent is informed may be particularly significant as it may mean that the data subject must be properly informed of the particular risk arising from his/her data being transferred to a country lacking adequate protection. The Commissioner points in the Guide to the definition of consent in the Directive and states that consent will not be valid if the individual has no choice but to give consent.

There are clearly "grey areas" relating to consent and the extent to which it is "freely given", "specific" and "informed". A job applicant, for example, applying for a job with a multinational company and being asked for consent to the transfer of his/her personal data overseas to a country with an "inadequate" data protection regime is not readily going to refuse such consent, and both the Article 29 Working Party and the UK Commissioner in guidance on employment matters have indicated their view that such consent may not be "freely given".

The Working Party suggests that the "consent" exemption could be useful in cases where the transferor has direct contact with the data subject and where the necessary information could be easily provided and unambiguous consent obtained.

CONTRACTUAL REQUIREMENTS

8–53 A number of the exemptions require that the transfer be "necessary" for the relevant reason or purpose. It must be borne in mind that the term imports a test of proportionality. The use of the term and its importance are considered in Ch.5 on the grounds for processing. The second exemption covers transfers necessary for the performance of a contract between the data subject and the controller (or the implementation of pre–contractual measures taken in response to the data subject's request).

[65] Sch.1 Pt 2 para.14.

Thus a data controller relying upon this condition to will only also be able to do so transfer personal data overseas if the contract relied upon is between the data controller and data subject.

The third exemption covers transfers necessary for the conclusion or performance of a contract concluded in the interest of the data subject and entered into at the request of the data subject between the controller and a third party.

The second and third exemptions appear potentially quite wide, but their application in practice is likely to be limited by the "necessity test": all of the data transferred must be necessary for the performance of the contract. Thus if additional non-essential data are transferred or if the purpose of the transfer is not the performance of the contract but rather some other purpose (follow-up marketing, for example) the exemption will be lost. With respect to pre-contractual situations, this would only include situations initiated by the data subject (such as a request for information about a particular service) and not those resulting from marketing approaches made by the data controller.

In spite of these caveats, these second and third exemptions are not without impact. They are applicable, for example, to those transfers necessary to reserve an airline ticket for a passenger or to transfers of personal data necessary for the operation of an international bank or credit card payment. Indeed, art.26(1)(c) of the Directive provides that the exemption for contracts "in the interest of the data subject" specifically covers the transfer of data about the beneficiaries of bank payments, who, although data subjects, may often not be party to a contract with the transferring controller.

Substantial public interest

The fourth exemption permits transfers which are necessary for reasons of substantial public interest. **8–54**

The Working Party suggests that this may cover certain limited transfers between public administrations, although they warn that care must be taken not to interpret this provision too widely. A simple public interest justification for a transfer does not suffice, it must be a question of substantial public interest.

Recital 58, upon which the exemptions are based, actually provides that there should be an exemption:

> "where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services—competent for social security matters."

This clearly suggests, therefore, that data transfers between tax or customs administrations or between services responsible for social security will generally be covered. Transfers between supervisory bodies in the financial services sector may also benefit from the exemption.

The fourth exemption contains a provision for the Secretary of State to specify by order when relevant transfers are and are not to be taken as necessary for reasons of substantial public interest.

The Immigration and Asylum Act 1999 provides that, for the purposes of para.4(1) of Sch.4, the provision of identification data under s.13 is a transfer of personal data which is necessary for reasons of substantial public interest. The

section applies where a person is to be removed from the UK to a country of which he is not a national or a citizen, but will not be admitted unless identity data relating to him is provided by the Secretary of State. This appears to be the only time the power has been exercised. The Home Office discussion documents on subordinate legislation did not contain any proposals for such orders.

Legal proceedings

8–55 The fifth exemption covers transfers which are necessary in connection with legal proceedings, for obtaining legal advice, or for establishing, exercising or defending legal rights.

This exemption is identical to the sixth condition for the legitimate processing of sensitive data. Its terms are discussed at Ch.5. Clearly, again, the satisfaction of this condition for the legitimate processing of sensitive data will also permit the cross-border transfer of such data without consideration of the restrictions in the eighth principle.

The data subject's vital interests

8–56 The sixth exemption concerns transfers necessary in order to protect the vital interests of the data subject. An obvious example of such a transfer would be the urgent transfer of medical records to a third country where a tourist who had previously received medical treatment in the EU has suffered an accident or has become dangerously ill.

It should be borne in mind, however, that the phrase "vital interests" is not without problems. This exemption is of course identical to the fourth condition for legitimate processing contained in Sch.2. Its terms are discussed at Ch.5. Yet again, the satisfaction of this condition for the legitimate processing of sensitive data will also "passport" the cross-border transfer of such data without consideration of the restrictions in the eighth principle.

In the Guide the Commissioner emphasises the view that this exemption may only be relied on where the data transfer relates to matters of life and death.

Public registers

8–57 The seventh exemption concerns transfers made from registers intended by law for consultation by the public, provided that in the particular case the conditions for consultation are fulfilled. The Working Party suggest that the intention of this exemption is that where a register in a Member State is available for public consultation or by persons demonstrating a legitimate interest, then the fact that the person who has the right to consult the register is actually situated in a third country, and that the act of consultation in fact involves a data transfer, should not prevent the information being transmitted to him.

Recital 58 of the Directive qualifies the exemption in the following manner:

> "where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation

by persons having a legitimate interest—the transfer should be made only at the request of those persons or if they are to be the recipients."

Thus the Directive makes it clear that entire registers or entire categories of data from registers should not be permitted to be transferred under this exemption. Given these restrictions, this exemption should not be considered to be a general exemption for the transfer of public register data. For example, it is reasonably clear that mass transfers of public register data for commercial purposes or the trawling of publicly available data for the purpose of profiling specific individuals would not benefit from the exemption.

The authority of the Commissioner

The eighth and ninth exemptions empower the Commissioner to authorise or approve certain types of cross-border transfers of personal data. The exemptions permit such transfers when: **8–58**

(a) the transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects; or
(b) the transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

The Commissioner issued formal approval of the EU approved contractual terms under para.8. It is also possible for data controllers to seek such approval of contractual terms or authorisation for particular transfers by application to the Commissioner as well as for the Commissioner to issue such approval or authority on his own initiative after conducting his own investigations.

The Commissioner must consider any applications made by or on behalf of exporting controllers for approval or authorisation under paras 8 or 9, respectively, of Sch.4 of the Act. However, exporting controllers should note that in the past such references have not been not encouraged for individual contracts although consent will be given to the adoption of Binding Corporate Rules under this power.

Contract clauses and authorisations

Any approvals or authorisations by the Commissioner must be referred to the Commission and other Member States for EU-wide approval or rejection in accordance with paras 2–4 of art.26 of the Directive. Section 54(7) of the 1998 Act provides: **8–59**

"The Commissioner shall inform the European Commission and the supervisory authorities in other EEA States:

(a) of any approvals granted for the purposes of paragraph 8 of Schedule 4.
(b) of any authorisations granted for the purposes of paragraph 9 of that Schedule."

Accordingly the UK Act does not require that data controllers who make their own assessment of adequacy or establish their own set of contractual protections submit anything to the Commissioner for authorisation. This contrasts with the position in many other Member States. As noted earlier the Commission has raised the question of whether the UK is meeting its obligations under the Directive given the reluctance of the regulator to approve individual contractual arrangements.

The basic prohibition on transfer to third countries which do not provide an adequate means of protection is found in art.25(1). Article 25(2) sets out the considerations which are relevant to a finding of adequacy. The remainder of the Article provides for determinations of adequacy by the Commission or Member States. It is silent on the question of whether a data controller is entitled to make its own determination on the issue. Article 26 provides for derogations, among them art.26(2) which provides that:

> "Without prejudice to paragraph 1, a Member State may authorise a transfer or set of transfers of personal data to a third country which does not ensure adequate protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses"

Member States must inform the Commission of any such authorisations. Although the Commission has criticised those countries which accept self assessment of adequacy by controllers and lamented the generally low level of authorisations notified to it, it has stopped short of threatening infraction proceedings.

ENFORCEMENT

8–60 Enforcement of the provisions relating to cross-border transfers is by way of the Commissioner serving an enforcement notice in accordance with s.40 of the 1998 Act. For a detailed discussion of the Commissioner's powers of enforcement, see Ch.20.

Impact of the draft Regulation in brief[66]

8–61 Under Ch.V art.40, any transfers of personal data which are undergoing processing or intended for processing after transfer to third countries or international organisations, are prohibited unless the conditions laid down in the Chapter, including onward transfers from one third country or international organisation to another, are met (plus the other provisions of the Regulation) by the controller and processor.

8–62 The conditions for transfer are a Commission adequacy finding; the controller or processor has adduced appropriate safeguards which include Binding Corporate Rules (BCRs) or can rely on a derogation. An adequacy finding may

[66] See Ch.1 paras 1-68 onwards for an overview of the draft Regulation as at January 2012.

relate to an international organisation, third country, or particular territory or processing sector within a third country (art.41). Member States may no longer make adequacy findings. Existing decisions made under Directive 95/46/EC remain in force until amended, replaced or repealed. In determining adequacy the Commission must take account of legislation and the "rule of law", including public security, defence, national security and professional rules, and security measures as well as the existence of supervisory authorities and effective redress and enforceable rights of individuals and the international commitments the third country or international organisation has entered into. Where a decision on adequacy is made the Commission must specify its geographical and sectoral application and, where there is an independent authority, the identity of that authority. The Commission may also decide that a country or territory does not offer an adequate level of protection but in such a case the data controller may still rely on the provisions in arts 42–44 to make transfers.

Article 42 sets out five appropriate safeguards which can be relied upon by a controller or a processor where there is no finding of adequacy: (i) BCRs in accord with art.43; (ii) standard contractual clauses adopted by the Commission; (iii) standard contractual clauses adopted by a supervisory authority in accordance with the consistency mechanism which have been declared valid by the Commission; (iv) individual contractual clauses authorised by the supervisory authority; and (v) individual authorisation by the supervisory authority. Where supervisory authorities seek to adopt standard clauses they must go through the consistency mechanism and also be approved by the Commission. In effect, this allows supervisory authorities to introduce standard clauses for consideration. Although the wording of art.42(1) states that processors or controllers may only transfer if appropriate safeguards are adduced in a "legally binding instrument", in fact art.42(5) allows for transfers to be approved where there is no legally binding instrument in place. **8–63**

Where controllers or processors rely on BCRs or Commission adopted or approved standard contractual clauses (authorised clauses), no further authorisations (such as permits) are required for transfers to take place. In the cases in which the controller or processor wishes to use contractual clauses other than authorised clauses they must be submitted to the supervisory authority for prior authorisation. If the transfer is based on such contractual clauses and

> "related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union",

the consistency procedure is set in motion. If the contractual clauses do not affect data subjects in another or other Member States or free movement they can be approved by the supervisory authority to which they are submitted. In the absence of a legally binding instrument, the controller or processor may obtain prior authorisation for the transfer or set of transfers from the supervisory authority "or for provisions to be inserted into administrative arrangements providing the basis of such transfer" under art.34. If the transfer is

188

> "related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union",

the consistency procedure is set in motion.

8–64 Article 43 sets out the provisions on BCRs. BCRs that meet the requirements of art.43 may be approved by a supervisory authority but must first pass the consistency procedure. The Commission has reserve powers to make delegated acts in relation to BCRs to specify the criteria and requirements and also the criteria for approval. BCRs may be adopted by processors.

8–65 Where no adequacy decision exists and appropriate safeguards have not been adduced, art.44 sets out eight permitted derogations:

(i) informed consent;
(ii) necessary for the performance of a contract between the data subject and the controller, or pre-contractual steps taken at the data subject's request;
(iii) necessary for the conclusion or performance of a contract between the controller and a third party, concluded in the data subject's interest;
(iv) necessary on important public interest grounds;
(v) necessary for the establishment, exercise or defence of legal claims;
(vi) necessary to protect the vital interests of the data subject or of another person, where the data subject is incapable of giving consent;
(vii) the transfer is made from a public register; or
(viii) necessary for the purposes of the legitimate interests pursued by the controller or processor which involve transfers which cannot be qualified as frequent or massive, and the controller or processor has assessed all the circumstances surrounding the transfer and where necessary adduced appropriate safeguards.

The derogations reflect those permitted under Directive 95/46/EC; however, they add the provision that a transfer may be made where it is necessary for the purposes of the legitimate interests pursued by the controller or processor, as long as these transfers are infrequent and not massive and safeguards have been adduced for the transfer. This is, however, very constrained as the controller must document the assessment as well as the safeguards and also notify the transfer to the supervisory authority. Public bodies cannot rely on the derogation on contractual grounds for transfer or legitimate interest. There are also restrictions on the use of the public interest test which must be "recognised in law" of the Union or the Member State. The Commission has the power to further specify what falls within this criteria. As it restricts the public interest ground to matters which are specified in the law of the Union or Member State a legal obligation in another jurisdiction is not sufficient to provide a ground for transfer. There is therefore a significant extension from art.25 of 95/46/EC in that the restriction on transfers will cover international organisations which will include ones based in the EU; the conditions will cover onward transfers of personal data; and data processors will be covered by the prohibition.

Additional materials

Directive 95/46/EC art.25 (transfer of personal data to third countries). **8–66**

8–67

Hansard references

Vol.586, No.108, CWH 25, Lords Grand Committee, February 23, 1998:
Adequacy, proposal that contracts should be included as part of programme to achieve adequacy rejected.
Vol.586, No.110, col.124, Lords Grand Committee, February 25, 1998:
Derogations.
Vol.586, No.110, cols 129, 130:
Data matching codes and preliminary assessment.
Commons Standing Committee D, June 4, 1998, col.317:
Transfers for reasons of substantial public interest.
Vol.315, No.198, col.576, Commons Third Reading, July 2, 1998:
Partial definition of transfer and a provision setting out the geographical scope of provisions in cl.5 withdrawn.

8–68

Case law

Lindqvist (C-101/01) [reference]:
reference to the European Court under art.234.

190

6

Sarah O'Toole

From: TRUSTe Feedback and Resolution System [consumer-feedback@feedback.truste.com]
Sent: 02 December 2013 20:54
To: Max Schrems
Subject: Re: TRUSTe #28321: www.facebook.com

Ticket #28321: www.facebook.com

Dear Maximilian Schrems,

TRUSTe Compliance 2, Dec 02 12:54 (PST):

Thank you for contacting TRUSTe. TRUSTe does not own or operate Facebook, though we do provide privacy-related dispute resolution services for Facebook.

As you may be aware, Facebook's privacy policy includes a notice to consumers that it may share consumer data as follows:

"We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm."

You requested the following resolution:
"Stop Facebook Inc's involvement in PRISM."

TRUSTe does not have authority to address the matter you raise. We are therefore closing this issue in our system as being outside the scope of TRUSTe's authority.

--TRUSTe Compliance Team

Sincerely,

TRUSTe Compliance Team

This email is a service from TRUSTe Feedback and Resolution System.

Message-Id:1BBDA49M_529cf37494d00_26ab3fd6150c67c0346672c3_sprut

7

The 'Safe Harbor' Privacy Principles as issued by the U.S Department of Commerce and agreed by the EU Commission pursuant to the EU Data Protection Directive provide that "adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization". Similar provisions are also contained in the model contracts approved by the EU Commission for the transfer of personal data to third countries.

We consider that an Irish-based data controller has met their data protection obligations in relation to the transfer of personal data to the U.S. if the U.S. based entity is 'Safe Harbor' registered. We further consider that the agreed 'Safe Harbor' Progamme envisages and addresses the access to personal data for law enforcement purposes held by a U.S. based data processor.

We are aware of and welcome the fact that the proportionality and oversight arrangements for programmes such as PRISM are to be the subject of high-level discussions between the EU and the USA. The issue was already raised by the (Irish) Minister for Justice in his meeting with the US Attorney-General on the occasion of the EU-US meeting on justice and law enforcement issues in mid-June (http://www.justice.ie/en/JELR/Pages/PR13000237).We also welcome the fact that the broader issue of the proper balance to be struck in a democratic society between the right to protection of personal data and measures to combat terrorism and serious crime - such as in relation to the Data Retention Directive and the activities of European intelligence services - are also receiving attention in the EU, notably in cases before the European Court of Justice and in the context of the negotiation of new data protection laws.

Finally, we would remind you that the Data Protection Commissioner has yet to receive from you a formal request for a decision in relation to the twenty two complaints previously made to this Office. In the absence of such a request, we must assume that you are now satisfied that actions taken by Facebook-Ireland in response to our audit have fully dealt with your complaints. If that is not the case, we would wish to uphold your right to receive formal decisions on these complaints as soon as possible, decisions that you may then appeal to the Courts if you so wish.

Yours sincerely,

[redacted]
Senior Compliance Officer

8

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

25 July 2013

Mag. Maximilian Schrems
[redacted]

Dear Mr. Schrems,

With reference to your letter of today's date, I am happy to clarify the points you raise.

Your recent Complaint ("complaint 23"):
In relation to the issue you have raised on the disclosure of personal data to US law enforcement authorities, my letter of 23 July 2013 and follow-up email of 24 July 2013 explained why we consider that this disclosure is permitted under Irish law and why we consider therefore that there is no reason to formally investigate this issue. During our phone conversation of 24 July, I repeatedly invited you to submit in writing any queries which you had and that I would arrange a reply to those queries. I did not confirm any of the points which are outlined in the first main paragraph of your letter where you reference that phone call.

Section 10 (1) (a) of the Data Protection Acts provides that the Commissioner *may investigate whether any of the provisions of (the) Act ... have, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.* As the Commissioner is satisfied that there is no evidence of a contravention in this case, he has exercised his discretion not to proceed to a formal investigation under section 10 (1) (b) of the Acts. In making this assessment, the Commissioner is also mindful of the fact that there is no evidence - and you have not asserted - that your personal data has been disclosed to the US authorities. The situation in this respect is quite different to that in relation to the 22 complaints you submitted earlier which related to terms and conditions of Facebook-Ireland which clearly apply to you as a user.

The right of the Commissioner not to proceed to a formal investigation of a complaint has recently been upheld by the Irish High Court in the cases of *Peter Nowak and the Data Protection Commissioner* [2012] IEHC 449] and *David Fox and the Office of the Data Protection Commissioner* [2013] IEHC 49 – both judgments available at www.courts.ie.

The requirement under Article 28.4 of the Data Protection Directive 95/46/EC, which is transposed by the Irish Acts, is that *...each supervisory authority shall hear claims lodged by any person.... concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.* We consider that this requirement has been met in relation to your "claim".

193

If you wish to contest the Commissioner's assessment of the law, you are free to seek judicial review in the Irish High Court.

Your other Complaints:
You and your organisation have consistently maintained that the Commissioner has failed in his duty to uphold Irish and EU law in relation to the processing of personal data by Facebook-Ireland and have repeated this claim to the European Commission, the European Parliament and in public statements. In your letter to us – which you published on your website – you referred to "previous – so far undecided – 22 complaints", with the implication that we have refused or delayed making such decisions and are thus failing in our legal duty.

Lest there be any further doubt on this issue, the Commissioner wishes to see your complaints finalised as soon as possible. If you are not satisfied that some or all of these complaints have been "amicably resolved" in the context of our detailed audit of Facebook-Ireland (published on our website) - and you are free to reformulate your complaints or to submit fresh complaints if you wish – then you should seek formal decisions from the Commissioner. If you were not happy with these decisions, you would be free to appeal them to the Irish Courts and to seek referral of any disputed points of EU law to the European Court of Justice. Your failure to date to seek such decisions after such a long delay could reasonably lead to a conclusion that you no longer considered them to be valid, hence the reference in my letter.

We have explained to you repeatedly that we follow exactly the same procedure in relation to your complaints as we do in all other complaints we receive. The Data Protection Acts oblige the Commissioner to seek an amicable resolution to any such complaints in an ombudsman-type role. Our procedures are therefore informal and not those of a court. We ensure that both parties have a clear understanding of the issues in dispute without giving direct access to source documentation.

In most cases, we manage to achieve an amicable resolution. In cases where this cannot be achieved between the parties to the complaint – and this may be the case in relation to some or all of your complaints – then the Commissioner issues a formal decision as to whether or not he considers there has been a breach of the Data Protection Acts. Such decisions can be appealed to the Circuit Court - and to higher (and European) courts on points of law - where the more formal procedures of a court apply.

I hope that this letter clarifies the points you have raised. You may also consider it useful to publish this letter in full on your website, together with the letter I addressed to you in relation to Facebook-Ireland.

Yours sincerely,

[redacted]
Senior Compliance Officer

9

Court of Justice of the European Union

Regina (NS (Afghanistan)) *v* Secretary of State for the Home Department (Amnesty International Ltd and others intervening)

E and others *v* Refugee Applications Commissioner and another (Amnesty International Ltd and others intervening)

(Joined Cases C-411/10 and C-493/10)

2011 June 28; Sept 22; Dec 21

President V Skouris, Presidents of Chambers A Tizzano, J N Cunha Rodrigues, K Lenaerts, J-C Bonichot, J Malenovský, U Lõhmus, Judges A Rosas, M Ilešič, T von Danwitz, A Arabadjiev, C Toader, J J Kasel

Advocate General V Trstenjak

European Union — Immigration — Asylum — Third country nationals entering United Kingdom and Ireland via Greece and seeking asylum — Greece member state responsible for examining asylum applications — Asylum seekers requesting United Kingdom and Ireland to exercise right to examine asylum applications themselves rather than return them to Greece — Whether member state implementing European Union law when deciding whether to exercise right to examine asylum application itself — Whether lawful for member state to apply conclusive presumption that asylum seeker's fundamental rights would be respected in member state responsible — Whether member state obliged to examine asylum application itself where transfer exposing asylum seeker to violation of fundamental rights — Whether scope of protection of fundamental rights wider under European Union law than under Human Rights Convention — Whether provision of national law designating member state responsible safe country unlikely to refoule asylum seekers contravening asylum seeker's rights to effective remedy and fair trial — Whether obligations of United Kingdom affected by opt-out from Charter of Fundamental Rights of European Union — EU Treaty, art 6EU, Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom, art 1(1) — Council Regulation (EC) No 343/2003, art 3(1)(2) — Charter of Fundamental Rights of the European Union, arts 1, 14, 18, 47, 51 — Convention for the Protection of Human Rights and Fundamental Freedoms (1953) (Cmd 8969), art 3

In the first case the claimant, an Afghan national, arrived in the United Kingdom via Greece and sought asylum. Taking the view that Greece was the member state responsible for examining the claimant's asylum application, pursuant to the criteria set out in Chapter III of Council Regulation (EC) No 343/2003[1], the Home Secretary called upon Greece, pursuant to article 17 of the Regulation, to take charge of the claimant in order to examine his application. Upon its failure to respond to that request within the two-month time limit stipulated by article 18(7) of the Regulation, Greece was deemed to have accepted responsibility for examining the claimant's application. Subsequently the Home Secretary issued directions for the claimant's removal to Greece, certifying under the Asylum and Immigration (Treatment of Claimants, etc) Act 2004 that the claimant's assertion that his removal to Greece

[1] Council Regulation (EC) No 343/2003, art 3: see post, opinion, para 20.

195

A would violate his human rights was unfounded since Greece was on the list of safe countries in Schedule 3 to the 2004 Act. The claimant then requested the Home Secretary to exercise her discretion under article 3(2) of the Regulation to examine the claimant's asylum application, contending that there was a risk that his fundamental rights under, inter alia, European Union law and the Convention for the Protection of Human Rights and Fundamental Freedoms[2] would be breached if he were returned to Greece, but the Home Secretary refused to do so. The claimant's
B claim for judicial review of the Home Secretary's decisions was dismissed and he appealed to the Court of Appeal.

In the second case the five claimants, variously nationals of Afghanistan, Iran and Algeria, came to Ireland via Greece and sought asylum. They brought proceedings in the High Court of Ireland, challenging decisions to return them to Greece on the grounds that the procedures and conditions for asylum seekers in Greece were inadequate and that Ireland was therefore required to exercise its right under
C article 3(2) of Council Regulation (EC) No 343/2003 to examine their asylum applications.

The Court of Appeal and the High Court of Ireland respectively, referred to the Court of Justice of the European Union questions asking whether, and if so in what circumstances, a member state would be required to exercise its right under article 3(2) of the Regulation to examine an application for asylum which was not its responsibility if it were established that transfer to the member state which was
D primarily responsible would expose the asylum seeker to a risk of violation of his fundamental rights, or whether it could be presumed that another member state would observe an asylum seeker's fundamental rights. The Court of Appeal additionally referred questions asking whether (i) a member state's decision whether to exercise its discretion under article 3(2) fell within the scope of European Union law for the purposes of article 6EU of the EU Treaty[3] and article 51 of the Charter of Fundamental Rights of the European Union[4]; (ii) the scope of the protection which
E articles 1, 18 and 47 of the Charter conferred on a person to whom the Regulation applied was wider than the protection conferred by article 3 of the Human Rights Convention and (iii) the answers to any of the questions referred were qualified by Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom, annexed to the EU Treaty.

On the references—

Held, (1) that when a member state made a decision on the basis of article 3(2) of
F Regulation No 343/2003 whether to examine an asylum application which was not its responsibility according to the criteria laid down in Chapter III of that Regulation it was implementing European Union law for the purposes of article 6EU of the EU Treaty and article 51 of the Charter of Fundamental Rights of the European Union, and so it was required to observe the fundamental rights set out in the Charter when making its decision (post, judgment, paras 68, 69, operative part, para 1).

(2) That, although the Common European Asylum System of which Council
G Regulation (EC) No 343/2003 formed a part had been conceived on the assumption that all the participating states observed fundamental rights, European Union law precluded the application of a conclusive presumption that the member state which

[2] Convention for the Protection of Human Rights and Fundamental Freedoms, art 3: "No one shall be subjected to torture or to inhuman or degrading treatment or punishment."

[3] EU Treaty, art 6(1)EU: "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties."

H Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom, art 1: see post, opinion, para 15.

[4] Charter of Fundamental Rights of the European Union, art 1: see post, opinion, para 8.
Art 4: see post, opinion, para 9.
Art 18: see post, opinion, para 10.
Art 47: see post, opinion, para 12.
Art 51: see post, opinion, para 13.

article 3(1) of the Regulation indicated as responsible observed the fundamental rights of the European Union; that article 4 of the Charter precluded member states, including the national courts, from transferring an asylum seeker to the member state responsible for the purposes of article 3(1) of the Regulation where they could not be unaware that systemic deficiencies in the asylum procedure and in the reception conditions of asylum seekers in that member state amounted to substantial grounds for believing that the asylum seeker would face a real risk of being subjected to inhuman or degrading treatment within the meaning of article 4 of the Charter; that where a member state found that it was impossible to transfer an asylum seeker to the member state responsible it should, subject to the right to examine the application itself under article 3(2) of the Regulation, examine the criteria set out in Chapter III of the Regulation in order to establish whether one of them enabled another member state to be identified as responsible for the examination of the asylum application; and that the member state in which the asylum seeker was present had to ensure that it did not worsen a situation where the fundamental rights of that applicant had been infringed by using a procedure for determining the member state responsible which took an unreasonable length of time, if necessary itself examining the application in accordance with the procedure laid down in article 3(2) of the Regulation (post, judgment, paras 86, 94, 96, 98, 99, 105–108, operative part, para 2).

(3) That the protection which was conferred on a person to whom Regulation No 343/2003 applied by the rights set out in articles 1, 18 and 47 of the Charter, concerning human dignity, the right to asylum and the right to an effective remedy, was no wider than the protection conferred by the right not to be subjected to torture or to inhuman or degrading treatment or punishment, guaranteed by article 3 of the Convention for the Protection of Human Rights and Fundamental Freedoms; and that, therefore, articles 1, 18 and 47 of the Charter did not lead to a different approach in such cases (post, judgment, paras 114–115, operative part, para 3).

(4) That, article 1(1) of Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom (whereby the Charter did not extend the ability of the Court of Justice or any United Kingdom court to find that United Kingdom law was inconsistent with the fundamental rights, freedoms and principles which the Charter affirmed) did not exempt the United Kingdom from the obligation to comply with the Charter's provisions or prevent an United Kingdom court from ensuring compliance with them; and that, accordingly, the approach to be taken in such cases by the United Kingdom did not require to be qualified in any respect so as to take account of that Protocol (post, judgment, paras 120, 122, operative part, para 4).

The following cases are referred to in the judgment:

Abdulla v Bundesrepublik Deutschland (Joined Cases C-175/08, C-176/08, C-178/08 and C-179/08) [2011] QB 46; [2010] 3 WLR 1624; [2010] All ER (EC) 799; [2010] ECR I-1493, ECJ

Bolbol v Bevándorlási és Állampolgársági Hivatal (Case C-31/09) [2012] All ER (EC) 469; [2010] ECR I-5539, ECJ

Chakroun v Minister van Buitenlandse Zaken (Case C-578/08) [2010] ECR I-1839, ECJ

Elliniki Radiophonia Tiléorassi AE v Dimotiki Etairia Pliroforissis (Case C-260/89) [1991] ECR I-2925, ECJ

KRS v United Kingdom (2008) 48 EHRR SE 129

Lindqvist, Criminal proceedings against (Case C-101/01) [2004] QB 1014; [2004] 2 WLR 1385; [2004] All ER (EC) 561; [2003] ECR I-12971, ECJ

MSS v Belgium and Greece (2011) 53 EHRR 28, GC

McB v E (Case C-400/10PPU) [2011] Fam 364; [2011] 3 WLR 699; [2011] All ER (EC) 379, ECJ

Ordre des barreaux francophones et germanophone v Conseil des ministres (Conseil des Barreaux de l'Union européene intervening) (Case C-305/05) [2007] All ER (EC) 953; [2007] ECR I-5305, ECJ
Wachauf v Federal Republic of Germany (Case 5/88) [1989] ECR 2609, ECJ

The following additional cases are referred to in the opinion of the Advocate General in Case C-411/10:

Bulicke v Deutsche Büro Service GmbH (Case C-246/09) [2010] ECR I-7003, ECJ
Detiček v Sgueglia (Case C-403/09PPU) [2010] Fam 104; [2010] 3 WLR 1098; [2010] All ER (EC) 313; [2009] ECR I-12193, ECJ
Elgafaji v Staatssecretaris van Justitie (Case C-465/07) [2009] 1 WLR 2100; [2009] All ER (EC) 651; [2009] ECR I-921, ECJ
European Parliament v Council of the European Union (Commission of the European Communities intervening) (Case C-540/03) [2007] All ER (EC) 193; [2006] ECR I-5769, ECJ
Germany, Federal Republic of v B (Joined Cases C-57/09 and C-101/09) [2012] 1 WLR 1076, ECJ
Karlsson (Case C-292/97) [2000] ECR I-2737, ECJ
Kudla v Poland (2000) 35 EHRR 198, GC
Migrationsverket v Petrosian (Case C-19/08) [2009] ECR I-495, ECJ
Tyrer v United Kingdom (1978) 2 EHRR 1
Unibet (London) Ltd v Justitiekanslern (Case C-432/05) [2008] All ER (EC) 453; [2007] ECR I-2271, ECJ
V v United Kingdom (1999) 30 EHRR 121, GC
Van der Weerd v Minister van Landbouw, Natuur en Voedselkwaliteit (Joined Cases C-222/05 to C-225/05) [2007] ECR I-4233, ECJ
Volker & Markus Schecke GbR v Land Hessen (Bundesanstalt für Landwirtschaft und Ernährung, joint party) (Joined Cases C-92/09 to C-93/09) [2012] All ER (EC) 127, ECJ
Willy Kempter KG v Hauptzollamt Hamburg-Jonas (Case C-2/06) [2008] ECR I-411, ECJ

R (NS (Afghanistan)) v Secretary of State for the Home Department (Amnesty International Ltd and others intervening) (Case C-411/10)

REFERENCE from the Court of Appeal

By an order dated 12 July 2010, on an appeal from a decision of the High Court to dismiss a claim, brought by the claimant, NS, an Afghan national, for judicial review by way of an order to quash decisions of the defendant, the Secretary of State for the Home Department, to issue directions for his removal to Greece and not to exercise her discretion under article 3(2) of Council Regulation (EC) No 343/2003 to examine his asylum application, the Court of Appeal [2010] EWCA Civ 990 referred to the Court of Justice of the European Union seven questions, post, judgment, para 50, concerning the interpretation of article 3(2) of Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the member state responsible for examining an asylum application lodged in one of the member states by a third country national (OJ 2003 L50, p 1), of articles 1, 4, 18 and 47 of the Charter of Fundamental Rights of the European Union (OJ 2010 C83, p 389) and of Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom (OJ 2010 C83, p 313). Amnesty International Ltd, the AIRE Centre, the United Nations High Commissioner for Refugees and the Equality and Human Rights Commission intervened in the proceedings.

By orders of 19 November 2010 and 16 May 2011 by the President of the Court of Justice the case was joined with Case C-493/10 for the purposes of the written and oral procedure and the judgment.

The judge rapporteur was Judge Rosas.

The facts are stated in the judgment.

E and others v Refugee Applications Commissioner and another (Amnesty International Ltd and others intervening) (Case C-493/10)

REFERENCE from the High Court, Ireland

By an order dated 11 October 2010, in proceedings between the claimants, E, M, T, P and H, and the defendants, the Refugee Applications Commissioner and the Minister for Justice Equality and Law Reform, the High Court (Ireland) referred to the Court of Justice of the European Union two questions, post, judgment, para 53, concerning the interpretation of article 3(2) of Council Regulation (EC) No 343/2003. Amnesty International Ltd, the AIRE Centre and the United Nations High Commissioner for Refugees intervened in the proceedings.

By orders of 19 November 2010 and 16 May 2011 by the President of the Court of Justice the case was joined with Case C-411/10 for the purposes of the written and oral procedure and the judgment.

The judge rapporteur was Judge Rosas.

The facts are stated in the judgment.

Dinah Rose QC, *Mark Henderson* and *Alison Pickup* (instructed by *Solicitor, Immigration Advisory Service*) for the claimant in the first case.

C Power, *F McDonagh* and *G Searson* for the claimants in the second case.

Simon Cox, *Sharam Taghavi*, *J Tomkin* (instructed by *Open Society Justice Initiative*) for Amnesty International Ltd and the AIRE Centre in the first case.

B Shipsey and *J Tomkin* for Amnesty International Ltd and the AIRE Centre in the second case.

Geoffrey Robertson QC for the Equality and Human Rights Commission.

Raza Husain QC, *Samantha Knights* and *Marie Demetriou* (instructed by *Baker & McKenzie*) for the United Nations High Commissioner for Refugees.

D O'Hagan, agent, *S Moorhead* and *D Conlan Smyth* for Ireland.

C Murrell, agent, and *Daniel Beard* (instructed by *Treasury Solicitor*) for the United Kingdom Government.

C Pochet and *T Maternethe*, agents, for the Belgian Government.

M Smolek and *J Vláčil*, agents, for the Czech Government.

T Henze and *N Graf Vitzthum*, agents, for the German Government.

A Samoni-Rantou, *M Michelogiannaki*, *T Papadopoulou*, *F Dedousi* and *M Germani*, agents, for the Government of Greece.

G de Bergues, *E Belliard* and *B Beaupère-Manokha*, agents, for the French Government.

G Palmieri, agent, and *M Russo*, for the Italian Government.

C M Wissels and *M Noort*, agents, for the Netherlands Government.

G Hesse, agent, for the Austrian Government.

M Arciszewski, *B Majczyna* and *M Szpunar*, agents, for the Polish Government.

N Aleš Verdir and *V Klemenc*, agents, for the Slovenian Government.

J Heliskoski, agent, for the Finnish Government.

M Condou-Durande, *M Wilderspin* and *H Kraemer*, agents, for the European Commission.

O Kjelsen, agent, for the Swiss Confederation.

22 September 2011. **ADVOCATE GENERAL V TRSTENJAK** delivered the following opinion in Case C-411/10.

Table of contents

200

I—Introduction

1 One of the greatest challenges in creating the Common European Asylum System is establishing a fair, but also effective distribution of the burden, associated with immigration, on the asylum systems of the European Union member states. This is illustrated particularly clearly by the present reference for a preliminary ruling, in which the referring court asks the Court of Justice to clarify the way in which the overloading of a member state's asylum system affects the European Union arrangements for determining the member states responsible for asylum applications lodged in the European Union.

2 The criteria for determining the member state responsible for an asylum application lodged in the European Union are laid down in Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the member state responsible for examining an asylum application lodged in one of the member states by a third country national (OJ 2003 L50, p 1). A fundamental characteristic of the system for allocating responsibilities in asylum cases introduced by that Regulation is that, in principle, a single member state is responsible for each asylum application lodged in the European Union. Where a third country national has applied for asylum in a member state which is not primarily responsible for examining that application under Regulation No 343/2003, the Regulation provides for mechanisms for the transfer of the asylum seeker to the member state which is primarily responsible.

3 However, in the light of the current crisis affecting the Greek asylum system, the question arises, for the other member states, whether asylum

A seekers may be transferred to Greece pursuant to Regulation No 343/2003 for the purpose of examining their asylum applications if it cannot be guaranteed that those asylum seekers will be treated and their applications will be examined in Greece in accordance with the Charter of Fundamental Rights of the European Union (OJ 2010 C83 p 389) ("the Charter") and the Convention for the Protection of Human Rights and Fundamental Freedoms
B ("the ECHR"). Because article 3(2) of Regulation No 343/2003 accords the member states the right, by way of derogation from the normal rules on responsibility, to take on the examination of an asylum application lodged in their territory, rather than the member state which is primarily responsible, the question also arises whether the member states' right to assume responsibility for the examination themselves may become a duty to assume responsibility for the examination if there is a risk that the asylum seeker's
C fundamental rights and human rights will be violated if he is transferred to the member state which is primarily responsible.

4 The referring court must rule on these questions in the main proceedings, in which an Afghan asylum seeker is challenging his return from the United Kingdom to Greece. Against this background, the referring court essentially asks whether, and if so in what circumstances, the United
D Kingdom may be required under European Union law, in a case like the main proceedings, to assume responsibility for examining asylum applications itself, even though Greece is primarily responsible for the examinations under Regulation No 343/2003.

5 Because the Charter has particular relevance in this connection, the referring court also requests clarification about the content and scope of
E Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom ("Protocol No 30").

6 In answering the questions referred, regard must also be had to the judgment of the European Court of Human Rights in *MSS v Belgium and Greece* (2011) 53 EHRR 28—which was delivered after the order for reference had been made—in which the European Court of Human Rights
F considered the transfer of an Afghan asylum seeker from Belgium to Greece to be a violation by Belgium of articles 3 and 13 of the ECHR.

7 Furthermore, the present case is closely connected with *E v Refugee Applications Comr (Amnesty International Ltd intervening)* (Case C-493/10) in which I deliver my opinion on the same day as in the present case. In *E's* case the central issue is the transfer of asylum seekers from
G Ireland to Greece pursuant to Regulation No 343/2003 and that case has been joined with the present case, by order of the President of the Court of Justice, for the purposes of the written and oral procedure and the judgment. For reasons of clarity, however, I am delivering separate opinions in the present case and in *E's* case.

H *II—Legislative framework*

A—European Union law

1. Charter of Fundamental Rights

8 Article 1 of the Charter provides, under the heading "Human dignity": "Human dignity is inviolable. It must be respected and protected."

9 Article 4 of the Charter provides, under the heading "Prohibition of torture and inhuman or degrading treatment or punishment": "No one shall be subjected to torture or to inhuman or degrading treatment or punishment."

10 Article 18 of the Charter provides, under the heading "Right to asylum":

> "The right to asylum shall be guaranteed with due respect for the rules of the Geneva Convention of 28 July 1951 and the Protocol of 31 January 1967 relating to the status of refugees and in accordance with the Treaty on European Union and the Treaty on the Functioning of the European Union."

11 Article 19 of the Charter provides, under the heading "Protection in the event of removal, expulsion or extradition":

> "1. Collective expulsions are prohibited.
>
> "2. No one may be removed, expelled or extradited to a state where there is a serious risk that he or she would be subjected to the death penalty, torture or other inhuman or degrading treatment or punishment."

12 Article 47 of the Charter provides, under the heading "Right to an effective remedy and to a fair trial":

> "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice."

13 Article 51 of the Charter provides, under the heading "Field of application":

> "1. The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the member states only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.
>
> "2. The Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties."

14 Article 52 of the Charter provides, under the heading "Scope of guaranteed rights":

> "1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of

A proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

"2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties.

B "3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

"7. The explanations drawn up as a way of providing guidance in the C interpretation of this Charter shall be given due regard by the courts of the Union and of the member states."

2. Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom

15 Protocol (No 30) on the application of the Charter of Fundamental D Rights of the European Union to Poland and to the United Kingdom, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, has two articles which read as follows:

"*Article 1*

"1. The Charter does not extend the ability of the Court of Justice of the European Union, or any court or tribunal of Poland or of the United E Kingdom, to find that the laws, regulations or administrative provisions, practices or action of Poland or of the United Kingdom are inconsistent with the fundamental rights, freedoms and principles that it reaffirms.

"2. In particular, and for the avoidance of doubt, nothing in Title IV of the Charter creates justiciable rights applicable to Poland or the United F Kingdom except in so far as Poland or the United Kingdom has provided for such rights in its national law.

"*Article 2*

"To the extent that a provision of the Charter refers to national laws and practices, it shall only apply to Poland or the United Kingdom to the extent that the rights or principles that it contains are recognised in the law or practices of Poland or of the United Kingdom."

G

3. Secondary law

16 The European Council, at its special meeting in Tampere on 15 and 16 October 1999, agreed to work towards establishing a Common European Asylum System, based on the full and inclusive application of the Convention Relating to the Status of Refugees, signed in Geneva on 28 July H 1951 (Cmd 9171) as amended by the Protocol relating to the Status of Refugees adopted on 31 January 1967 (1967) (Cmnd 3906) ("the Geneva Convention"), thus affirming the principle of non-refoulement and ensuring that nobody is sent back to persecution. At that special meeting, the European Council also acknowledged the need to reach agreement on the

issue of temporary protection for displaced persons on the basis of solidarity between member states.

17 The measures adopted to implement the Tampere Conclusions included the following Regulation and the following Directives[1*]:

—Regulation No 343/2003,

—Council Directive 2001/55/EC of 20 July 2001 on minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between member states in receiving such persons and bearing the consequences thereof (OJ 2001 L212, p 12)

—Council Directive 2003/9/EC of 27 January 2003 laying down minimum standards for the reception of asylum seekers (OJ 2003 L31, p 18)

—Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted (OJ 2004 L304, p 12)

—Council Directive 2005/85/EC of 1 December 2005 on minimum standards on procedures in member states for granting and withdrawing refugee status (OJ 2005 L326, p 13).

18 That Regulation and those Directives specifically provide as follows:

(a) Regulation No 343/2003

19 In article 1, Regulation No 343/2003 lays down the criteria and mechanisms for determining the member state responsible for examining an application for asylum lodged in one of the member states by a third country national.

20 Article 3 of Regulation No 343/2003 states:

"1. Member states shall examine the application of any third country national who applies at the border or in their territory to any one of them for asylum. The application shall be examined by a single member state, which shall be the one which the criteria set out in Chapter III indicate is responsible.

"2. By way of derogation from paragraph 1, each member state may examine an application for asylum lodged with it by a third country national, even if such examination is not its responsibility under the criteria laid down in this Regulation. In such an event, that member state shall become the member state responsible within the meaning of this Regulation and shall assume the obligations associated with that responsibility. Where appropriate, it shall inform the member state previously responsible, the member state conducting a procedure for determining the member state responsible or the member state which has been requested to take charge of or take back the applicant.

"3. Any member state shall retain the right, pursuant to its national laws, to send an asylum seeker to a third country, in compliance with the provisions of the Geneva Convention.

* *Reporter's note.* The superior figures in the text refer to notes which can be found at the end of the Advocate General's opinion, on pp 143–148.

A "4. The asylum seeker shall be informed in writing in a language that he or she may reasonably be expected to understand regarding the application of this Regulation, its time limits and its effects."

21 Article 4 of Regulation No 343/2003 states:

"1. The process of determining the member state responsible under this
B Regulation shall start as soon as an application for asylum is first lodged with a member state.

"2. An application for asylum shall be deemed to have been lodged once a form submitted by the applicant for asylum or a report prepared by the authorities has reached the competent authorities of the member state concerned. Where an application is not made in writing, the time
C elapsing between the statement of intention and the preparation of a report should be as short as possible."

22 Article 5 of Regulation No 343/2003 provides:

"1. The criteria for determining the member state responsible shall be applied in the order in which they are set out in this Chapter.

"2. The member state responsible in accordance with the criteria shall
D be determined on the basis of the situation obtaining when the asylum seeker first lodged his application with a member state."

23 Article 10 of Regulation No 343/2003 states:

"1. Where it is established, on the basis of proof or circumstantial evidence as described in the two lists mentioned in article 18(3), including
E the data referred to in Chapter III of Regulation (EC) No 2725/2000, that an asylum seeker has irregularly crossed the border into a member state by land, sea or air having come from a third country, the member state thus entered shall be responsible for examining the application for asylum. This responsibility shall cease 12 months after the date on which the irregular border crossing took place.

F "2. When a member state cannot or can no longer be held responsible in accordance with paragraph 1, and where it is established, on the basis of proof or circumstantial evidence as described in the two lists mentioned in article 18(3), that the asylum seeker—who has entered the territories of the member states irregularly or whose circumstances of entry cannot be established—at the time of lodging the application has
G been previously living for a continuous period of at least five months in a member state, that member state shall be responsible for examining the application for asylum. If the applicant has been living for periods of time of at least five months in several member states, the member state where this has been most recently the case shall be responsible for examining the application."

H 24 Article 13 of Regulation No 343/2003 provides:

"Where no member state responsible for examining the application for asylum can be designated on the basis of the criteria listed in this Regulation, the first member state with which the application for asylum was lodged shall be responsible for examining it."

25 Article 16 of Regulation No 343/2003 states:

"1. The member state responsible for examining an application for asylum under this Regulation shall be obliged to: (a) take charge, under the conditions laid down in articles 17 to 19, of an asylum seeker who has lodged an application in a different member state; (b) complete the examination of the application for asylum; . . ."

"3. The obligations specified in paragraph 1 shall cease where the third country national has left the territory of the member states for at least three months, unless the third country national is in possession of a valid residence document issued by the member state responsible."

26 Article 17(1) of Regulation No 343/2003 provides:

"Where a member state with which an application for asylum has been lodged considers that another member state is responsible for examining the application, it may, as quickly as possible and in any case within three months of the date on which the application was lodged within the meaning of article 4(2), call upon the other member state to take charge of the applicant. Where the request to take charge of an applicant is not made within the period of three months, responsibility for examining the application for asylum shall lie with the member state in which the application was lodged."

27 Article 18 of Regulation No 343/2003 states:

"1. The requested member state shall make the necessary checks, and shall give a decision on the request to take charge of an applicant within two months of the date on which the request was received."

"7. Failure to act within the two-month period mentioned in paragraph 1 and the one-month period mentioned in paragraph 6 shall be tantamount to accepting the request, and entail the obligation to take charge of the person, including the provisions for proper arrangements for arrival."

28 Article 19 of Regulation No 343/2003 provides:

"1. Where the requested member state accepts that it should take charge of an applicant, the member state in which the application for asylum was lodged shall notify the applicant of the decision not to examine the application, and of the obligation to transfer the applicant to the responsible member state.

"2. The decision referred to in paragraph 1 shall set out the grounds on which it is based. It shall contain details of the time limit for carrying out the transfer and shall, if necessary, contain information on the place and date at which the applicant should appear, if he is travelling to the member state responsible by his own means. This decision may be subject to an appeal or a review. Appeal or review concerning this decision shall not suspend the implementation of the transfer unless the courts or competent bodies so decide on a case-by-case basis if national legislation allows for this.

"3. The transfer of the applicant from the member state in which the application for asylum was lodged to the member state responsible shall be carried out in accordance with the national law of the first member

A state, after consultation between the member states concerned, as soon as practically possible, and at the latest within six months of acceptance of the request that charge be taken or of the decision on an appeal or review where there is a suspensive effect . . .

"4. Where the transfer does not take place within the six months' time limit, responsibility shall lie with the member state in which the
B application for asylum was lodged. This time limit may be extended up to a maximum of one year if the transfer could not be carried out due to imprisonment of the asylum seeker or up to a maximum of 18 months if the asylum seeker absconds."

(b) Directive 2001/55

29 According to article 1, the purpose of Directive 2001/55 is to
C establish minimum standards for giving temporary protection in the event of a mass influx of displaced persons from third countries who are unable to return to their country of origin and to promote a balance of effort between member states in receiving and bearing the consequences of receiving such persons.

30 Under article 2(a) of Directive 2001/55,"temporary protection"
D means a procedure of exceptional character to provide, in the event of a mass influx or imminent mass influx of displaced persons from third countries who are unable to return to their country of origin, immediate and temporary protection to such persons, in particular if there is also a risk that the asylum system will be unable to process this influx without adverse effects for its efficient operation, in the interests of the persons concerned and other persons requesting protection.

E 31 Chapter II of Directive 2001/55 contains rules on the duration and implementation of temporary protection. Chapter III concerns the obligations of the member states towards persons enjoying temporary protection. Chapter IV of the Directive regulates access to the asylum procedure in the context of temporary protection. Chapter V of the Directive concerns return and measures after temporary protection.
F Chapter VI concerns the distribution of burdens and responsibilities among the member states in the spirit of solidarity within the European Union.

(c) Directive 2003/9

32 Article 1 states that the purpose of Directive 2003/9 is to lay down minimum standards for the reception of asylum seekers in member states.

33 The minimum standards laid down in Directive 2003/9 relate to the
G member states' information duties vis-à-vis asylum seekers (article 5), provision of documentation for asylum seekers (article 6), residence and freedom of movement for asylum seekers (article 7), the preservation of family unity for asylum seekers (article 8), schooling and education of minors (article 10), access to the labour market for asylum seekers (article 11), vocational training (article 12) and material reception
H conditions and health care for asylum seekers: article 13 et seq.

34 Article 21 of Directive 2003/9 provides, under the heading "Appeals":

"1. Member states shall ensure that negative decisions relating to the granting of benefits under this Directive or decisions taken under article 7

208

which individually affect asylum seekers may be the subject of an appeal within the procedures laid down in the national law. At least in the last instance the possibility of an appeal or a review before a judicial body shall be granted.

"2. Procedures for access to legal assistance in such cases shall be laid down in national law."

35 Under article 23 of Directive 2003/9, member states must, with due respect to their constitutional structure, ensure that appropriate guidance, monitoring and control of the level of reception conditions are established. Under article 24(2), member states must allocate the necessary resources in connection with the national provisions enacted to implement that Directive.

(d) Directive 2004/83

36 Under article 1 of Directive 2004/83, the purpose of the Directive is to lay down minimum standards for the qualification of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted.

37 Chapters II, III and V of Directive 2004/83 contain a number of rules and criteria relating to the assessment of applications for the granting of refugee status or for the granting of subsidiary protection status and relating to the qualification of third country nationals as refugees or as persons eligible for subsidiary protection. Chapter IV contains, first, a provision under which member states must grant refugee status to a third country national or a stateless person who qualifies as a refugee in accordance with Chapters II and III: article 13. Secondly, that Chapter lays down detailed rules on revocation of, ending of or refusal to renew refugee status: article 14. Chapter VI contains the relevant rules on the granting of subsidiary protection status (article 18) and on the revocation of, ending of or refusal to renew subsidiary protection status: article 19. Chapter VII lays down the content of international protection, including protection from refoulement: article 21. Chapter VIII governs matters of administrative co-operation. Under article 36, member states must ensure, among other things, that authorities and other organisations implementing the Directive have received the necessary training.

(e) Directive 2005/85

38 Under article 1 of Directive 2005/85, the purpose of the Directive is to establish minimum standards on procedures in member states for granting and withdrawing refugee status.

39 Under article 3(1) of Directive 2005/85, the Directive applies to all applications for asylum made in the territry, including at the border or in the transit zones of the member states, and to the withdrawal of refugee status. The first sub-paragraph of article 4(1) provides that member states must designate for all procedures a determining authority which will be responsible for an appropriate examination of the applications in accordance with the Directive.

40 The basic principles underlying those procedures and the guarantees to be given to asylum seekers in this connection are laid down in Chapter II of Directive 2005/85. Specific rules on the procedures for granting refugee

A status are contained in Chapter III of the Directive, which also introduces the safe third country concept (article 27) and the safe country of origin concept: article 31. Chapter V includes rules on the right of asylum seekers to an effective remedy: article 39.

B—International law

B 1. Convention Relating to the Status of Refugees

41 Under article 33(1) of the Geneva Convention, no contracting state may expel or return ("refouler") a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion.

C 2. European Convention for the Protection of Human Rights and Fundamental Freedoms

42 Under article 3 of the ECHR, no one may be subjected to torture or to inhuman or degrading treatment or punishment.

43 Under article 13 of the ECHR, everyone whose rights and freedoms as set forth in the Convention are violated must have an effective remedy D before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

III—Facts and reference for a preliminary ruling

44 In the main proceedings, the referring court has to decide on an appeal brought by an Afghan asylum seeker ("the claimant") against a E decision of the High Court of Justice of England and Wales, Queen's Bench Division (Administrative Court), by which the claimant challenges his transfer to Greece by the United Kingdom. The respondent in the main proceedings, the Secretary of State for the Home Department, is the Government minister with responsibility for immigration and asylum in the United Kingdom.

F 45 On his journey from Afghanistan to the United Kingdom, the claimant travelled through, among other countries, Greece, where he was arrested and fingerprinted on 24 September 2008. He did not claim asylum in Greece. Following detention in that member state, he was ordered to leave Greece within 30 days and was subsequently expelled to Turkey. Having escaped from detention in Turkey, he made his way to the United Kingdom, where he arrived on 12 January 2009 and applied for asylum on G that same date.

46 On 1 April 2009, the Secretary of State requested Greece, pursuant to Regulation No 343/2003, to take charge of the claimant. Following failure by the Greek authorities to respond within the period laid down by Regulation No 343/2003, Greece was deemed to have accepted responsibility under that Regulation for consideration of the claim.

H 47 The claimant was informed on 30 July 2009 that he would be removed to Greece on 6 August 2009. On 31 July 2009 the Secretary of State notified him of a decision taken under the Asylum and Immigration (Treatment of Claimants, etc) Act 2004 certifying that his claim that removal to Greece would violate his rights under the ECHR was clearly unfounded. The effect of that decision was that the claimant did not have a

right, under national law, to appeal against the decision to remove him to Greece, to which he would otherwise have been entitled.

48 Following an unsuccessful request that the Secretary of State accept responsibility for determining his asylum claim pursuant to article 3(2) of Regulation No 343/2003 inter alia on the ground that his fundamental rights under European Union law would be breached in the event of his return to Greece, the claimant was informed, on 4 August 2009, that the Secretary of State was maintaining the decision to remove him to Greece.

49 On 6 August 2009, the claimant issued a claim for judicial review of the decision to certify that his claim under the ECHR was unfounded and of the decision to remove him to Greece. As a result of this claim, the directions which had been made to remove him to Greece were cancelled by the Secretary of State.

50 In view of the importance of the issues raised, on 14 October 2009 the Administrative Court granted the claimant permission to bring his claim for judicial review, it being ordered that his case should become the lead case in England and Wales on returns to Greece under Regulation No 343/2003.

51 By judgment of 31 March 2010, the Administrative Court dismissed the claim by the claimant, but granted him permission to appeal to the referring court in view of the general importance of the issues raised.

52 The referring court concluded that the treatment of the appeal raises fundamental questions regarding the scope of article 3 of Regulation No 343/2003 and the effect on that article of rights which the claimant claims under the Charter and under international Conventions such as the ECHR.

53 Against this background, the referring court stayed the main proceedings and made reference to the Court of Justice for a preliminary ruling on the following questions: [the questions are set out, post, judgment, para 50.

IV—Procedure before the court

54 The order for reference dated 12 July 2010 was lodged at the Registry of the Court of Justice on 18 August 2010. In its order for reference, the referring court requested, pursuant to article 104b(1) of the Rules of Procedure, that the reference for a preliminary ruling be dealt with under the urgent procedure. By an order of the President of the Court of Justice of 1 October 2010, that request was rejected.

55 By order of the President of the Court of Justice of 9 November 2010, Cases C-411/10 and C-493/10 were joined for the purposes of the written procedure and, by order of the President of the Court of Justice of 16 May 2011, for the purposes of the oral procedure and the judgment.

56 In the written procedure, observations were submitted by the claimant, Amnesty International Ltd ("Amnesty") and the AIRE (Advice on Individual Rights in Europe) Centre, the United Nations High Commissioner for Refugees ("the UNHCR") and the Equality and Human Rights Commission ("the EHRC"), as interveners in the main proceedings, the Kingdom of Belgium, the Federal Republic of Germany, the Republic of Finland, the French Republic, the Hellenic Republic, Ireland, the Italian Republic, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Poland, the United Kingdom, the Czech Republic, the Swiss

A Confederation and the Commission of the European Union. The representatives of the appellant, Amnesty and the AIRE Centre, the UNHCR and the Equality and Human Rights Commission, the Republic of Slovenia, the French Republic, the Hellenic Republic, Ireland, the Kingdom of the Netherlands, the Republic of Poland, the United Kingdom and the European Commission ("the commission") took part at the hearing on
B 28 June 2011.

V—Arguments of the parties

57 The first question, which asks whether a decision made by a member state under article 3(2) of Regulation No 343/2003 whether to examine a claim for asylum falls within the scope of European Union law, must be
C answered in the affirmative in the view of the commission, the Finnish, French and Netherlands Governments, the claimant, the UNHCR, Amnesty and the AIRE Centre, and the EHRC. In the view of the Austrian Government too, the European Union fundamental rights are applicable to a decision made by a member state whether to exercise its right to assume responsibility for the examination itself under article 3(2) of Regulation No 343/2003.

D 58 In the view of Ireland and the Italian, United Kingdom and Belgian Governments, on the other hand, the decision on the exercise of the right to assume responsibility for the examination under article 3(2) of Regulation No 343/2003 does not fall within the scope of European Union law. The Belgian Government adds a significant qualification to its statement, however, pointing out that the transfer of an asylum seeker to the member
E state primarily responsible under Regulation No 343/2003 does fall within the scope of European Union law.

59 In answering the first question, the Czech Government differentiates between the case where a member state exercises the right to assume responsibility for the examination itself under article 3(2) of Regulation No 343/2003 and the case where it does not exercise that right. Only the decision to exercise the right to assume responsibility for the examination
F under article 3(2) falls within the scope of European Union law. On the other hand, the non-exercise of the right to assume responsibility for the examination under article 3(2) does not fall within the scope of European Union law.

60 The German Government does not comment expressly on the first question and answers the other questions in case the court were to conclude
G that the exercise of discretion in article 3(2) of Regulation No 343/2003 should be regarded as "implementing Union law" within the meaning of the first sentence of article 51(1) of the Charter.

61 In answering the second, third and fourth questions, the commission, the Finnish, French, German and Netherlands Governments, the United Kingdom Government [2] and the Belgian Government, the claimant and the UNHCR essentially take the view that, in the context of the
H application of Regulation No 343/2003, the rebuttable presumption may be made that the member state responsible for examining an asylum application will act in accordance with European Union law and international law. However, in so far as it should be established in a specific case that the transfer of the asylum seeker to the member state which is

primarily responsible and the treatment of the asylum seeker in that member state would violate the rights enshrined in the Charter, the transferring member state is required, in the view of the commission, the Finnish, French, Belgian and United Kingdom Governments, the claimant, the UNHCR, Amnesty and the AIRE Centre, to exercise its right to assume responsibility for the examination itself under article 3(2) of Regulation No 343/2003. In the view of the German and the Netherlands Governments, an asylum seeker may no longer be transferred to the member state which is primarily responsible in such a case.

62 The United Kingdom Government also stresses that an obligation to exercise the right to assume responsibility for the examination may arise only under extraordinary circumstances, namely where the presumption that the responsible member state will act in accordance with humans rights and European Union law vis-à-vis a certain category of asylum seekers has been clearly rebutted and the asylum seeker comes under that category.

63 In the view of the Swiss Confederation[3], Regulation No 343/2003 inherently contains a rebuttable presumption that the participating states will comply with the Geneva Convention and the ECHR. However, where that presumption is rebutted in a specific case and it is not guaranteed that the asylum seeker will be treated in accordance with international law in the responsible state, a transfer to that state is precluded and the right to assume responsibility for the examination under article 3(2) of Regulation No 343/2003 exceptionally becomes a duty.

64 In the view of the Italian, Polish, Slovenian and Greek Governments and Ireland, on the other hand, it is not possible to infer from article 3(2) of Regulation No 343/2003 a duty to exercise the right to assume responsibility for the examination. In the view of the Greek, Slovenian and Polish Governments, moreover, under European Union law a member state may not review the conformity with European Union law of the action of another member state.

65 In answer to the fifth question, the United Kingdom, Italian and Netherlands Governments argue that the scope of the protection conferred on a person to whom Regulation No 343/2003 applies by the rights set out in articles 1, 18 and 47 of the Charter is not wider than the protection conferred by article 3 of the ECHR. The claimant, the EHRC, the UNHCR, Amnesty and the AIRE Centre claim, on the other hand, that the protection of an asylum seeker to be transferred on the basis of the Charter and the general principles of European Union law extends further than the protection guaranteed by article 3 of the ECHR.

66 In the view of the German Government, the European Union fundamental rights stemming from articles 4 and 19(2) of the Charter correspond to the fundamental right under article 3 of the ECHR. Article 18 of the Charter does not contain a right to guaranteed asylum, but to protection against removal in accordance with article 33 of the Geneva Convention. The scope of article 47 of the Charter is wider than that of articles 6 and 13 of the ECHR in so far as the first paragraph requires a judicial remedy and the second paragraph is not restricted to civil and criminal proceedings.

67 In answer to the sixth question, the commission, the Netherlands Government, the claimant, the UNHCR, Amnesty and the AIRE Centre argue that a national law imposing a conclusive presumption that each

A member state is a safe country from which the asylum seeker will not be sent to another state in contravention of his rights pursuant to the ECHR and the Geneva Convention is incompatible with article 47 of the Charter. The United Kingdom Government stresses that this presumption may be considered to be rebutted only in the case of manifest violations of fundamental rights and human rights. The Italian Government, on the other B hand, takes the view that a conclusive presumption applying in national law, according to which the other member states are safe countries, is compatible with article 47 of the Charter.

68 In answer to the seventh question, the commission, the Polish Government, the United Kingdom Government, the claimant, the UNHCR, the EHRC, Amnesty and the AIRE Centre argue that the provisions of Protocol No 30 do not affect their proposed answers to the questions C referred.

VI—Legal assessment

A—First question

69 By its first question, which asks whether a decision made by a D member state, pursuant to its right to assume responsibility for the examination under article 3(2) of Regulation No 343/2003, to examine a claim for asylum, rather than the member state which is primarily responsible, falls within the scope of European Union law for the purposes of article 6EU of the EU Treaty (post-Lisbon) and/or article 51 of the Charter, the referring court is essentially seeking to ascertain whether, and if so in what circumstances, the member states must comply with the E provisions of the Charter in deciding whether to exercise their right to assume responsibility for the examination under article 3(2) of Regulation No 343/2003[4].

70 The answer to this question should have regard to article 6(1)EU, which classifies the Charter as European Union primary law (first sub-paragraph) and also states that the provisions of the Charter do not F extend in any way the competences of the European Union as defined in the Treaties: second sub-paragraph. With regard to the specific interpretation and application of the Charter, the third sub-paragraph of article 6(1)EU refers to Title VII (articles 51 to 54) of the Charter.

71 Article 51 of the Charter defines the field of application of the Charter. Article 51 confirms, first of all, that the provisions of the Charter G are addressed to the institutions, bodies, offices and agencies of the European Union, and to the member states. Secondly, it is ensured that the binding force of fundamental rights for the European Union institutions and the member states does not have the effect of either shifting powers at the expense of the member states or extending the field of application of European Union law beyond the powers of the European Union as established in the Treaties[5].

H 72 In order to preclude an extension of the European Union's powers in relation to the member states, article 51(1) of the Charter provides in particular that

—the application of the Charter must not restrict the principle of subsidiarity (first sentence of article 51(1)),

214

—the member states are bound by the Charter only when they are implementing European Union law (first sentence of article 51(1)),

—the observance and application of the Charter must respect the limits of the powers of the European Union as conferred on it in the Treaties: second sentence of article 51(1).

73 In addition, article 51(2) of the Charter contains the general statement that the Charter does not extend the field of application of European Union law beyond the powers of the European Union or establish any new power or task for the European Union, or modify powers and tasks as defined in the Treaties.

74 Against this background, with its first question the referring court takes up the requirement laid down in the first sentence of article 51(1) of the Charter that the member states are bound by the Charter only when they are implementing European Union law. In this connection it asks whether the member states "are implementing Union law" within the meaning of that provision where they decide, on the basis of their discretion under article 3(2) of Regulation No 343/2003, whether or not to examine an asylum application instead of the member state which is primarily responsible.

75 In my view, this question must be answered in the affirmative.

76 As can be seen from the Explanations relating to the Charter of Fundamental Rights ("the Explanations") (OJ 2007 C303, p 32)[6], the principle laid down in the first sentence of article 51(1) of the Charter, according to which the member states are bound by the Charter only when they are implementing European Union law, is to be regarded as a confirmation of the court's previous case law on respect by the member states for the fundamental rights defined in the context of the European Union. The Explanations make express reference to the decisions of principle in *Wachauf v Federal Republic of Germany* (Case 5/88) [1989] ECR 2609 and *Elliniki Radiophonia Tiléorassi AE v Dimotiki Etairia Pliroforissis* (Case C-260/89) [1991] ECR I-2925 ("the *ERT* case") and to *Karlsson* (Case C-292/97) [2000] ECR I-2737. (The *Karlsson* judgment can be classified in the *Wachauf* line of case law.)

77 In the *Wachauf* case the court found that the requirements of the protection of fundamental rights are also binding on the member states when they implement European Union rules and the member states must, as far as possible, apply those rules in accordance with those requirements: see *Wachauf*, para 19. (That judgment was confirmed in *European Parliament v Council of the European Union (Commission of the European Communities intervening)* (Case C-540/03) [2006] ECR I-5769; [2007] All ER (EC) 193, para 104 et seq.) In the *ERT* case the court also found that restrictions of the fundamental freedoms made by the member states must satisfy the requirements of the protection of fundamental rights in the European Union legal order: see the *ERT* case [1991] ECR I-2925, para 41 et seq.

78 Having particular regard to the fact that the Explanations make reference to both the *Wachauf* case law and the *ERT* case law, the member states must be regarded as being bound by the Charter, under article 51(1) of the Charter, both when they implement European Union rules and in the context of national restrictions of the fundamental freedoms: see also C Ladenburger, article 51, in *Tettinger & Stern (eds), Kölner Gemeinschafts Kommentar zur Europäische Grundrechtecharta* (2006), p 759, para 22 et

215

seq; Carsten Nowak, in *Heselhaus & Nowak (eds), Handbuch der Europäischen Grundrechte* (2006), § 6, para 44 et seq.

79 Against this background, the question arises in the present case whether a decision made by a member state under article 3(2) of Regulation No 343/2003 whether to examine a claim for asylum is to be regarded, for the purposes of article 51(1) of the Charter and in the light of the *Wachauf* case law, as a national implementing measure for Regulation No 343/2003.

80 In my view, this question must be answered in the affirmative. The discretion enjoyed by the member state in making that decision does not preclude that assessment. Rather, the crucial factor is that Regulation No 343/2003 lays down exhaustive rules for determining the member state responsible for examining an asylum application. The option afforded to the member states to examine asylum applications pursuant to article 3(2) of Regulation No 343/2003 is an integral part of those rules, which is, inter alia, reflected in the fact that the Regulation lays down comprehensive rules governing the legal consequences of such a decision[7]. Consequently, decisions taken by the member states on the basis of article 3(2) of Regulation No 343/2003 are also to be regarded as implementing measures, despite the discretion available to them.

81 This view is confirmed in *Wachauf* (Case 5/88) [1989] ECR 2609, in which the court examined, among other things, the compatibility of individual provisions of Commission Regulation (EEC) No 1371/84 of 16 May 1984 laying down detailed rules for the application of the additional levy referred to in article 5c of Regulation (EEC) No 804/68 (OJ 1984 L132, p 11) with the requirements of the protection of fundamental rights in the European Union legal order. Regulation No 1371/84 conferred on the member states the power to give the lessee of a milk-producing farm, under certain circumstances, compensation for the definitive discontinuance of milk production at the end of the lease. In the main proceedings, a lessee brought an action because he had been refused such compensation, even though he had definitively closed the farm intended for milk production he had built up. Against this background, the court was required to rule, inter alia, on whether that refusal to grant compensation inevitably followed from Regulation No 1371/84 and whether it was consistent with the European Union fundamental rights which had been recognised as general principles of law. In its judgment, the court held, on the one hand, that the refusal to grant a departing lessee the compensation in question should be regarded as an infringement of the requirements of the protection of fundamental rights in the European Union legal order if he was deprived, without compensation, of the fruits of his labour and of his investments in the tenanted holding: see *Wachauf*, para 19. Because, however, Regulation No 1371/84 allowed the member states, specifically in these cases, a sufficient margin of appreciation in granting the lessees due compensation which was consistent with the requirements of the protection of fundamental rights, in the view of the court, the rules contained in the Regulation were to be regarded as consistent with the fundamental rights: see *Wachauf*, para 22 et seq

82 Even though in *Wachauf* the court addressed, first and foremost, the consistency of the contested Regulation with fundamental rights, it confirmed, at least implicitly, that the decisions by the member states to grant compensation to departing lessees, which are taken by the national

216

authorities on the basis of the discretion conferred by Regulation No 1371/84, must, as far as possible, be in accordance with the requirements of the protection of fundamental rights. The court thus confirmed, at the same time, that decisions made by the member states on the basis of the discretion available to them under European Union legislation are to be regarded as implementing measures for that European Union legislation for the purposes of protection of fundamental rights under European Union law: see also *European Parliament v Council of the European Union* (Case C-540/03) [2006] ECR I-5769, para 104.

83 In the light of the foregoing, the first question must be answered to the effect that a decision made by a member state under article 3(2) of Regulation No 343/2003 whether to examine a claim for asylum which is not its responsibility under the criteria set out in Chapter III of the Regulation constitutes a measure implementing European Union law for the purposes of article 51(1) of the Charter.

B—Second, third and fourth questions

84 It follows from my above observations that in their decision under article 3(2) of Regulation No 343/2003 whether to examine a claim for asylum for which another member state is primarily responsible under the criteria set out in Chapter III of the Regulation, the member states must comply with the Charter. By the second, third and fourth questions, the referring court essentially asks whether, and if so in what circumstances, the member states may be required, in the light of this need to comply with the Charter, to exercise their right to assume responsibility for the examination themselves under article 3(2) of Regulation No 343/2003 if it were established that transfer to the member state which is primarily responsible would expose the asylum seeker to a risk of violation of his fundamental rights and/or to a risk that that member state would not comply with its obligations under Directives 2003/9, 2004/83 and 2005/85.

85 The referring court asks these questions because it has clear evidence that there is a wide gulf between the European Union rules applicable to Greece as regards the organisation of its asylum system, on the one hand, and the actual treatment of asylum seekers in Greece, on the other, such that there may be a risk that asylum seekers' fundamental rights and human rights will be violated if they are transferred to Greece.

86 In order to gain a better understanding of these questions, I will first examine the asylum measures in secondary law which are relevant in the present case and the relationship between those measures and the Charter, the Geneva Convention and the ECHR. I will go on to consider the problems faced by the Greek asylum system at present. I will then address the question how the overloading of the Greek asylum system must be taken into consideration by the other member states when applying Regulation No 343/2003.

1. The asylum measures in secondary law and their relationship with the Charter, the Convention Relating to the Status of Refugees and the ECHR

(a) Enabling legal basis in primary law

87 The European Union's competences were extended to matters related to asylum seekers and refugees in the Treaty of Amsterdam of 1997,

217

A by which rule-making powers in relation to asylum, refugees, immigration and residence of third country nationals were transferred to the European Union. A new article 73k was inserted in the EC Treaty, as an enabling legal basis in primary law, which was subsequently renumbered as article 63EC.

88 In asylum matters, rule-making powers were transferred to the European Union on the proviso, laid down in article 63(1)EC, that the
B measures on asylum to be adopted by the European Union legislature must be in accordance with the Geneva Convention and the Protocol of 31 January 1967 relating to the status of refugees and other relevant treaties. The "other relevant treaties" include the ECHR. (A correct analysis is given by M Graßhof, in *Schwarze (ed), EU-Kommentar*, 2nd ed (2009), article 63(4)EC, para 4.) Furthermore, article 63(1)EC expressly provided that the power of harmonisation in asylum matters was limited to
C establishing minimum standards: see article 63(1)(b)(c)(d)EC.

(b) Directives 2001/55, 2003/9, 2004/83 and 2005/85

89 On the basis of this enabling legal basis in primary law, the European Union legislature adopted four Directives laying down minimum standards regarding various aspects of national asylum systems. The first Directive
D adopted was Directive 2001/55, which lays down, inter alia, minimum standards for giving temporary protection in the event of mass influxes. The other three Directives introduced common minimum standards for the reception of asylum seekers (Directive 2003/9), for the qualification of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection
E granted (Directive 2004/83), and for procedures in member states for granting and withdrawing refugee status (Directive 2005/85) in nearly all the member states[8].

90 In accordance with the primary law provisions of article 63(1)EC, under which the measures of secondary law adopted on that basis must comply with the Geneva Convention, the recitals in the Preambles to Directives 2003/9, 2004/83 and 2005/85 all make reference to the
F conclusion of the Tampere European Council, according to which the Common European Asylum System to be developed is to be based on the full and inclusive application of the Geneva Convention: see recital (2) in the Preambles to Directive 2003/9, Directive 2004/83 and Directive 2005/85. The recitals in the Preambles to those Directives also stress that the Directives respect the fundamental rights and observe the principles
G recognised by the Charter (see recital (5) in the Preamble to Directive 2003/9, recital (10) in the Preamble to Directive 2004/83, and recital (8) in the Preamble to Directive 2005/85) and that the member states are bound by the instruments of international law to which they are party with respect to the treatment of persons falling within the scope of those Directives: see recital (6) in the Preamble to Directive 2003/9, recital (11) in the Preamble to Directive 2004/83, and recital (9) in the Preamble to Directive 2005/85.
H 91 Directives 2003/9, 2004/83 and 2005/85 therefore contain substantive minimum standards with respect to the treatment of asylum seekers and the examination of their applications. Furthermore, article 24(2) of Directive 2003/9 expressly provides that member states must allocate the necessary resources to achieve the minimum standards for the

reception of asylum seekers laid down therein. Similarly, article 36 of Directive 2004/83 provides that member states must ensure that authorities and other organisations implementing the Directive have received the necessary training.

92 It is therefore ensured, from a legal point of view, that the treatment of asylum seekers and the examination of their applications in the member states, which must respect the minimum standards contained in Directives 2003/9, 2004/83 and 2005/85, in principle also comply with the requirements of the Charter, the Geneva Convention and the ECHR[9].

(c) Regulation No 343/2003

93 According to recital (3) in its Preamble, the aim of Regulation No 343/2003—adopted on the basis of article 63(1)EC—is to introduce a clear and workable method for determining the member state responsible for the examination of an asylum application lodged within the European Union[10]. According to recital (4), this method should be based on objective, fair criteria both for the member states and for the persons concerned and should make it possible to determine rapidly the member state responsible, so as to guarantee effective access to the asylum procedure and the rapid processing of asylum applications.

94 In order to achieve these objectives, which are also intended to prevent forum shopping by asylum seekers, Regulation No 343/2003 lays down a provision under which responsibility for examining an asylum application lodged in the European Union rests with a single member state, which is determined on the basis of objective criteria. Those objective criteria include, for example, the existence of a link, in relation to the law on asylum and foreign nationals, between the asylum seeker or a family member and a member state: see articles 6, 7, 8 and 9(1)(2) of Regulation No 343/2003. In the case of an illegal entry into the European Union, the member state of first entry is responsible for examining the asylum application under article 10 of Regulation No 343/2003. (However, that responsibility expires 12 months after the illegal entry.) Under article 16 of Regulation No 343/2003, the member state responsible for examining an application for asylum is obliged to take charge of an asylum seeker who has lodged an application in a different member state and to complete the examination of the application for asylum. (Accordingly, article 25(1) of Directive 2005/85 provides that member states are not required to examine whether the applicant qualifies as a refugee in accordance with Directive 2004/83 where they are required to do so in accordance with Regulation No 343/2003.) The mechanism for transferring asylum seekers is laid down in articles 17 to 19 of Regulation No 343/2003.

95 The system under Regulation No 343/2003 for determining the member state responsible for examining an asylum application and for the transfer of the asylum seeker to that member state does not expressly take into consideration any differences in the organisation or in the management of the asylum systems and asylum procedures in the different member states. Specific reference is made to the (expected) treatment of the asylum seeker in the member state primarily responsible for his asylum application neither in the context of fixing the criteria for determining the responsible member

A state nor in connection with the mechanism for the transfer of asylum seekers between the member states.

96 The absence of a specific reference to the treatment of the asylum seeker in the member state which is primarily responsible can be explained by the interaction between Regulation No 343/2003 and Directives 2003/9, 2004/83 and 2005/85 and by the interaction between that Regulation and
B obligations on the individual member states under international law. Because, under those Directives, the treatment of asylum seekers and the examination of their asylum applications must satisfy substantive minimum standards in each member state and because all the member states have acceded to the ECHR and to the Geneva Convention, it is ensured, from a legal point of view, that the treatment of asylum seekers in each member state satisfies the requirements of the Charter, the Geneva Convention and
C the ECHR: see point 92 of this opinion.

97 Seen from this perspective, neither the Charter nor the Geneva Convention or the ECHR preclude the system introduced by Regulation No 343/2003, which lays down the rules for determining the member state in which asylum seekers are to be received for the purpose of examining their asylum applications and for the transfer of asylum seekers to that member
D state without express reference to the specific organisation and management of the asylum system and asylum procedures there[11].

(d) Interim conclusion

98 In summary, it must be stated, in the light of the foregoing, that the rules of secondary law on the treatment of asylum seekers and on the
E examination of asylum applications which stem from the interaction between Directives 2003/9, 2004/83 and 2005/85 and Regulation No 343/2003 are, in principle, consistent with the provisions of the Charter, the Geneva Convention and the ECHR, both in their objective and in their legal structure.

2. The overloading of the Greek asylum system

F 99 Regulation No 343/2003 does not contain any express provision in the case that member states—on account of their geographical location for example—are faced with a number of asylum seekers exceeding the capacities of their asylum system, with the result that they can no longer, in practice, guarantee that those asylum seekers will be treated and their asylum applications will be reviewed in accordance with Directives 2003/9,
G 2004/83 and 2005/85 and with their obligations stemming from fundamental rights and from international law[12].

100 Such an urgent situation appears to have arisen in Greece.

101 A clear indication to this effect is provided by the judgment of the European Court of Human Rights in *MSS v Belgium and Greece* 53 EHRR 28, in which the European Court of Human Rights dealt with the case of an Afghan national who had illegally entered the European Union
H from Turkey via Greece, and had then been detained in Greece. Without applying for asylum there, he left Greece following his release and eventually applied for asylum in Belgium. Because, after examining the Afghan asylum seeker's particulars, the Belgian authorities for foreign nationals concluded that, on account of the illegal first entry by the asylum seeker, Greece was

responsible for examining his asylum application in accordance with article 3(1) in conjunction with article 10(1) of Regulation No 343/2003, Belgium instituted the procedure for the transfer of the asylum seeker to Greece pursuant to Regulation No 343/2003 and, on the conclusion of that procedure, transferred him to Greece. Before his transfer, however, the Afghan asylum seeker had lodged an application with the European Court of Human Rights.

102 In its judgment, the European Court of Human Rights found that the conditions of detention and the living conditions of the Afghan asylum seeker in Greece were to be regarded as a violation of article 3 of the ECHR. With reference to the deficiencies in the examination of the asylum seeker's application, the risk of direct or indirect refoulement to his home country without any serious examination of the merits of his asylum application, and the absence of an effective remedy, the European Court of Human Rights also established a violation of article 13 in conjunction with article 3 of the ECHR. It also found that Belgium had also violated article 3 of the ECHR because, by sending the Afghan asylum seeker back to Greece, it had exposed him to the risks linked to the identified deficiencies in the Greek asylum system, and to detention and living conditions that were in breach of article 3 of the ECHR. Lastly, the European Court of Human Rights also found that Belgium had violated article 13 in conjunction with article 3 of the ECHR.

103 The national courts of the individual member states have also taken a critical view of the Greek asylum system and of detention and living conditions for asylum seekers in Greece in the context of Regulation No 343/2003 and the transfer of asylum seekers to Greece. For example, in its judgment of 7 October 2010, Judgment No U694/10, available on the Internet in the Legal Information System of the Republic of Austria (http://www.ris.bka.gv.at), the Austrian Verfassungsgerichtshof (Constitutional Court) found, in connection with a review of the constitutionality of the transfer to Greece under Regulation No 343/2003 of an Afghan single woman with three children, that whilst there is, in principle, the possibility of state provision where vulnerable persons are returned to Greece in order to implement the asylum procedure, this cannot be automatically assumed without a specific individual assurance on the part of the competent authorities.

104 The findings of fact made by the lower court, which are reproduced by the referring court as the appeal court in the order for reference, give a similar picture. Furthermore, in its written observations in the present case, the commission pointed out that on 3 November 2009 it sent Greece a letter of formal notice under article 226EC and on 24 June 2010 a supplementary letter of formal notice, in which Greece was alleged, inter alia, to have infringed various provisions of Directives 2003/9, 2004/83 and 2005/85.

105 It follows from these findings that the Greek asylum system is under considerable pressure as a result of overloading, as a result of which it can no longer always be guaranteed that asylum seekers will be treated and their applications will be reviewed in accordance with Directives 2003/9, 2004/83 and 2005/85. Under these conditions, it cannot be ruled out that asylum seekers who are transferred from another member state to Greece in accordance with the rules and mechanisms under Regulation No 343/2003 will experience treatment, after their transfer, which is incompatible with the provisions of the Charter, the Geneva Convention and the ECHR.

A 3. Consideration of the overloading of the member states' asylum systems in connection with the application of Regulation No 343/2003

106 In the light of the overloading of the Greek asylum system and the effects of that overloading on the treatment of asylum seekers and on the examination of their applications, the referring court faces the question whether a member state may transfer an asylum seeker to Greece, having B regard to the provisions of Regulation No 343/2003, even if it were established that such a transfer would expose the asylum seeker to a risk of violation of his fundamental rights and human rights. The referring court expands on this question of principle in the second, third and fourth questions.

107 With the second and third questions, the referring court essentially asks the Court of Justice for clarification whether, in applying Regulation C No 343/2003, the member states may proceed from the conclusive presumption that, after the transfer of the asylum seeker, the member state responsible for examining an asylum application will observe both the minimum standards laid down in Directives 2003/9, 2004/83 and 2005/85 and the asylum seeker's fundamental rights (third question), with the result that a transfer of asylum seekers under Regulation No 343/2003 is always to D be regarded as compatible with European Union fundamental rights, regardless of the situation in the responsible state: second question.

108 In the event that these questions were to be answered in the negative, the referring court would like to know, with its fourth question, whether, and if so in what circumstances, a member state is obliged, in applying Regulation No 343/2003, to take responsibility for reviewing an asylum application under article 3(2) of that Regulation, where transfer to E the member state which is primarily responsible would expose the asylum seeker to a risk of violation of his fundamental rights and/or to a risk that the minimum standards set out in Directives 2003/9, 2004/83 and 2005/85 will not be applied to him.

109 I will begin by considering the fourth question. I will then turn to the second and third questions.

F

(a) Fourth question: The duty to exercise the right to assume responsibility for the examination under article 3(2) of Regulation No 343/2003 where transfer to the member state which is primarily responsible would expose the asylum seeker to a serious risk of violation of his fundamental rights

G (i) The problem of a serious risk of violation of fundamental rights where an asylum seeker is transferred to the member state which is primarily responsible

110 Should a member state be unable, for any reason, to comply with the rules of Directives 2003/9, 2004/83 or 2005/85 or its obligations under international law with regard to the treatment of asylum seekers or the examination of their asylum applications, there is a de facto risk that if H asylum seekers are transferred to that member state, they will be exposed to treatment which violates their fundamental rights and their human rights.

111 In this connection, there could be fears, for example, of violations of the right to respect for and protection of human dignity enshrined in article 1 of the Charter or of the prohibition of torture and inhuman or

222

degrading treatment contained in article 4 of the Charter in the member state which is primarily responsible[13]. A

112 If there were a serious risk in a member state of a violation of the human dignity within the meaning of article 1 of the Charter of the asylum seekers transferred there, or inhuman or degrading treatment within the meaning of article 4 of the Charter, the transfer of asylum seekers to that member state would also be incompatible with article 1 or article 4 of the Charter. Under article 1 of the Charter, human dignity must not only be "respected", but also "protected". Such a positive protective function is also inherent in article 4 of the Charter: see W Höfling, in *Tettinger & Stern (eds), Kölner Gemeinschafts Kommentar zur Europäische Grundrechtecharta*, article 4, p 273, para 3; D Borowsky, in *J Meyer (ed), Charta der Grundrechte der Europäischen Union*, 3rd ed (2011), article 4, para 20. In addition, article 19(2) of the Charter expressly provides in this connection that no one may be removed, expelled or extradited to a state where there is a serious risk that he or she would be subjected to the death penalty, torture or other inhuman or degrading treatment or punishment[14]. B C

113 The complete overloading of a member state's asylum system may also mean, in certain circumstances, that it is necessary to examine the compatibility of the transfer of an asylum seeker to that member state with article 18 of the Charter. D

114 Under article 18 of the Charter, the right to asylum is guaranteed with due respect for the rules of the Geneva Convention, the EU Treaty and the FEU Treaty[15]. One of the central elements of the Geneva Convention is the prohibition of direct or indirect expulsion or return of a refugee to a persecuting state laid down in article 33 of that Convention, the principle of non-refoulement. Even though the precise scope of this prohibition on return is disputed, it must be assumed that it grants refugees[16] not only protection from direct deportation to the persecuting state, but also protection from chain deportation, where a transfer is made to a state in which there is a risk of deportation to a persecuting state: see Sir Elihu Lauterpacht and Daniel Bethlehem in *Feller, Türk & Nicholson (eds), Refugee Protection in International Law* (2003), p 122; *Hailbronnner, Asyl- und Ausländerrecht*, 2nd ed (2008), para 655. E F

115 If the overloading of a member state's asylum system were to mean that the refugees in that member state were at risk of direct or indirect return to a persecuting state, article 18 of the Charter therefore prohibits the other member states from transferring refugees to that member state.

G

(ii) The duty to assume responsibility for the examination under article 3(2) of Regulation No 343/2003

116 It follows from my above observations that, first of all, the overloading of a member state's asylum system may result in an environment in which one or more of the asylum seekers' rights enshrined in the Charter may be violated. Secondly, I have concluded that the transfer of asylum seekers to a member state in which there is a serious risk of violation of the asylum seekers' fundamental rights is incompatible with the Charter. H

117 Against this background, the question arises whether Regulation No 343/2003 can be interpreted in such a way that transfers of asylum seekers which violate fundamental rights can be ruled out.

223

A 118 The fact that Regulation No 343/2003 must, as far as possible, be interpreted in a manner consistent with fundamental rights follows, first, from the court's settled case law, according to which the member states must make sure they do not rely on an interpretation of an instrument of secondary legislation which would be in conflict with the fundamental rights protected by the European Union legal order or with the other general
B principles of European Union law: see *Detiček v Sgueglia* (Case C-403/09PPU) [2010] Fam 104; [2009] ECR I-12193, para 34; *Ordre des barreaux francophones et germanophone v Conseil des ministres (Conseil des Barreaux de l'Union européene intervening)* (Case C-305/05) [2007] ECR I-5305; [2007] All ER (EC) 953, para 28; and *Criminal proceedings against Lindqvist* (Case C-101/01) [2004] QB 1014; [2003] ECR I-12971, para 87. Secondly, an interpretation of Regulation No 343/2003 in a
C manner consistent with fundamental rights is necessary in particular since it is expressly stated in article 63(1)EC, which serves as an enabling legal basis for that Regulation in primary law, that European Union measures on asylum must be in accordance with the Geneva Convention and with other relevant treaties[17]. Recital (15) in the Preamble to Regulation No 343/2003 also confirms that that Regulation observes the fundamental rights and
D principles which are acknowledged in the Charter[18].

119 In my view, article 3(2) of Regulation No 343/2003 allows the member states a margin of discretion which is sufficiently wide to enable them to apply that Regulation in a manner compatible with the requirements of the protection of fundamental rights where transfer to the member state which is primarily responsible would expose the asylum seeker to a serious
E risk of violation of his fundamental rights as enshrined in the Charter.

120 Article 3(2) of Regulation No 343/2003 accords the member states the right to examine the asylum application lodged by an asylum seeker in that member state even where, under article 3(1) in conjunction with the provisions contained in Chapter III of the Regulation, another member state is primarily responsible. Where a member state exercises this right to assume responsibility for the examination, it becomes the responsible
F member state under article 3(2) of Regulation No 343/2003, which must assume the obligations associated with that responsibility.

121 If transfer to the member state which is primarily responsible would expose the asylum seeker to a serious risk of violation of his fundamental rights as enshrined in the Charter, the member state in which the asylum seeker has lodged an asylum application can therefore eliminate
G that risk entirely by exercising its right to assume responsibility for the examination under article 3(2) of Regulation No 343/2003.

122 Taking particular account of the fact that the member states are required to apply Regulation No 343/2003 in a manner consistent with fundamental rights and that a transfer of asylum seekers to a member state in which there is a serious risk of violation of one or more fundamental rights of those asylum seekers must, as a rule, be regarded as an infringement of the
H Charter by the transferring member state, the member states are obliged, in my view, to exercise the right to assume responsibility for the examination themselves under article 3(2) of Regulation No 343/2003 where there is a risk in the member state which is primarily responsible of violation of the rights of the asylum seeker to be transferred, as enshrined in the Charter.

123 Serious risks of infringements of individual provisions of Directives 2003/9, 2004/83 and 2005/85 in the member state primarily responsible which do not also constitute a violation of the fundamental rights of the asylum seeker to be transferred, as enshrined in the Charter, are not sufficient, on the other hand, to create an obligation on the part of the transferring member state to exercise the right to assume responsibility for the examination itself under article 3(2) of Regulation No 343/2003.

124 It should be stated, first of all, in this connection that an interpretation of Regulation No 343/2003 in a manner consistent with fundamental rights cannot require the exercise of the right to assume responsibility for the examination under article 3(2) where the host member state infringes individual provisions of Directives 2003/9, 2004/83 or 2005/85, but without infringing the Charter. Furthermore, the transfer of an asylum seeker to a member state in which there is no risk of violation of the rights of that asylum seeker, as enshrined in the Charter, does not normally lead to an infringement of the Charter by the transferring member state.

125 Furthermore, it would be difficult to reconcile with the aims of Regulation No 343/2003 if any failure to comply with Directives 2003/9, 2004/83 or 2005/85 were sufficient to prevent the transfer of an asylum seeker to the member state which is primarily responsible[19]. Regulation No 343/2003 is intended to establish a clear and workable method for determining the member state responsible for the examination of an asylum application, which also makes it possible to determine rapidly the member state responsible: see recital (3) et seq in the Preamble to the Regulation. In order to achieve that objective, Regulation No 343/2003 lays down a provision under which responsibility for examining each asylum application lodged in the European Union rests with a single member state, which is determined on the basis of objective criteria. In the case of an illegal entry into the European Union, the member state of first entry is responsible for examining the asylum application under article 10 of Regulation No 343/2003.

126 If any failure to comply with individual provisions of Directives 2003/9, 2004/83 or 2005/85 on the part of the member state of illegal first entry were now to mean that the member state in which the asylum seeker lodged an asylum application was required to exercise its right to assume responsibility for the examination itself under article 3(2) of Regulation No 343/2003, a new, far-reaching exclusion criterion would be created, in addition to the objective criteria for determining the responsible member state laid down in Chapter III of the Regulation, under which even minor infringements of Directives 2003/9, 2004/83 or 2005/85 in individual member states could mean that those member states would be relieved of their responsibilities under Regulation No 343/2003 and the associated duties. This could result not only in the rules on responsibility formulated in Regulation No 343/2003 being completely undermined, but could also jeopardise the aim of those rules, which is to determine rapidly the member states responsible for examining asylum applications lodged in the European Union.

225

A (iii) Interim conclusion

127 In the light of foregoing, the fourth question asked by the referring court must be answered to the effect that a member state in which an asylum application has been lodged is obliged to exercise its right to examine that asylum application itself under article 3(2) of Regulation No 343/2003 where transfer to the member state primarily responsible under article 3(1) B in conjunction with the provisions contained in Chapter III of Regulation No 343/2003 would expose the asylum seeker to a serious risk of violation of his fundamental rights as enshrined in the Charter. Serious risks of infringements of individual provisions of Directives 2003/9, 2004/83 and 2005/85 in the member state primarily responsible which do not also constitute a violation of the fundamental rights of the asylum seeker to be transferred, as enshrined in the Charter, are not sufficient, on the other hand, C to create an obligation on the part of the transferring member state to exercise the right to assume responsibility for the examination itself under article 3(2) of Regulation No 343/2003.

(b) Second and third questions: Recourse to conclusive presumptions in the context of the exercise of the right to assume responsibility for the D examination under article 3(2) of Regulation No 343/2003

128 With the second and third questions, the referring court is seeking to ascertain whether, in applying Regulation No 343/2003, the member states may proceed from the conclusive presumption that, after the transfer of the asylum seeker, the member state primarily responsible for examining the asylum application will observe the minimum standards laid down in E Directives 2003/9, 2004/83 and 2005/85 and the asylum seeker's fundamental rights (third question), with the result that a transfer of asylum seekers under Regulation No 343/2003 is always to be regarded as compatible with European Union fundamental rights, regardless of the situation in the responsible state: second question.

129 In my view, these questions should be answered in the negative.

130 As I have already explained above, the risk that transfer of asylum F seekers to another member state for the purpose of examining their asylum applications will expose them de facto to treatment which violates fundamental rights and human rights can never be completely ruled out. If there were a serious risk of violation of the asylum seeker's rights, as enshrined in the Charter, in the member state primarily responsible for examining an asylum application, the member state in which that asylum G seeker has lodged his asylum application is obliged to exercise the right to assume responsibility for the examination itself under article 3(2) of Regulation No 343/2003.

131 It is immediately clear from these findings that an application of Regulation No 343/2003 on the basis of the conclusive presumption that the asylum seeker's fundamental rights will be observed in the member state primarily responsible for his application is incompatible with the member H state's duty to interpret and apply Regulation No 343/2003 in a manner consistent with fundamental rights: see point 118 of this opinion. In that case, the member state in which the asylum seeker has lodged his asylum application would never be obliged to exercise the right to assume responsibility for the examination itself under article 3(2) of Regulation

226

No 343/2003, and it could not therefore be ruled out that asylum seekers would be transferred to another member state despite the serious risk of violation of their rights as enshrined in the Charter.

132 For the same reason, an application of Regulation No 343/2003 on the basis of the conclusive presumption that all the minimum standards laid down in Directives 2003/9, 2004/83 and 2005/85 will be observed in the host member state must also be rejected as contrary to European Union law. The conclusive presumption that all the minimum standards laid down in Directives 2003/9, 2004/83 and 2005/85 will be observed is no different, in practice, from the conclusive presumption that the asylum seekers' fundamental rights, as enshrined in the Charter, will be observed in the member state which is primarily responsible.

133 This does not mean, however, that, the member states are barred, in principle, from proceeding from the rebuttable presumption, in applying Regulation No 343/2003, that the asylum seeker's human rights and fundamental rights will be observed in the member state primarily responsible for his application. It should be borne in mind in this connection that the treatment of asylum seekers and the examination of their applications under Directives 2003/9, 2004/83 and 2005/85 must satisfy substantive minimum standards in each member state and that all the member states must observe the Charter[20] and—as contracting states—the ECHR and the Geneva Convention. In view of the high level of protection which is thus (legally) ensured, it seems reasonable, in connection with the transfer of asylum seekers, to proceed from the rebuttable presumption that those asylum seekers will be treated in a manner consistent with human rights and fundamental rights in the member state which is primarily responsible[21]. Accordingly, recital (2) in the Preamble to Regulation No 343/2003 expressly states that member states, all respecting the principle of non-refoulement, are considered as safe countries for third country nationals[22].

134 If the member states were to decide to operate such a rebuttable presumption, however, they must observe the principle of effectiveness, according to which the realisation of the rights conferred by European Union law may not be rendered practically impossible or excessively difficult. (With regard to the principle of effectiveness, see *Bulicke v Deutsche Büro Service GmbH* (Case C-246/09) [2010] ECR I-7003, para 25; *Willy Kempter KG v Hauptzollamt Hamburg-Jonas* (Case C-2/06) [2008] ECR I-411, para 57; *Van der Weerd v Minister van Landbouw, Natuur en Voedselkwaliteit* (Joined Cases C-222/05 to C-225/05) [2007] ECR I-4233, para 28; and *Unibet (London) Ltd v Justitiekanslern* (Case C-432/05) [2007] ECR I-2271; [2008] All ER (EC) 453, para 43.)

135 If the member states thus decide to introduce the rebuttable presumption that the asylum seeker's human rights and fundamental rights will be observed in the member state which is primarily responsible, the asylum seekers must be given the possibility, procedurally, actually to rebut that presumption. Having regard to the principle of effectiveness, the specific form of the available evidence and the definition of the rules and principles governing the assessment of evidence are, in turn, a matter for the national legal orders of the individual member states.

136 In the light of foregoing, the second and third questions must be answered to the effect that the obligation to interpret Regulation

227

A No 343/2003 in a manner consistent with fundamental rights precludes the operation of a conclusive presumption according to which the member state primarily responsible for examining an asylum application will observe the asylum seeker's fundamental rights under European Union law and all the minimum standards laid down in Directives 2003/9, 2004/83 and 2005/85. The member states are not barred, on the other hand, from proceeding from
B the rebuttable presumption, in applying Regulation No 343/2003, that the asylum seeker's human rights and fundamental rights will be observed in the member state primarily responsible for his asylum application.

C—Fifth question: Relationship between the protection of asylum seekers under the Charter and their protection under the ECHR

C 137 By its fifth question, the referring court wishes to know whether articles 1, 18 and 47 of the Charter accord asylum seekers who are to be transferred to another member state in accordance with Regulation No 343/2003 a wider scope of protection than article 3 of the ECHR.

138 Although the referring court did not expressly examine the legal background to that question, the decision of the European Court of Human Rights in *KRS v United Kingdom* (2008) 48 EHRR SE 129 appears to have
D played an important role in its referral. In that decision, the European Court of Human Rights was required to decide on an application under the ECHR by an Iranian national who was to be transferred from the United Kingdom to Greece pursuant to Regulation No 343/2003. The Iranian asylum seeker considered that removal to Greece would infringe article 3 of the ECHR. In its decision of 2 December 2008, the European Court of
E Human Rights rejected that application as manifestly ill-founded.

139 At the time the order for reference was made, the referring court therefore faced the question of how it had to take into consideration the decision of the European Court of Human Rights in *KRS v United Kingdom*. It had to be clarified whether the view taken by the European Court of Human Rights, that the transfer of an Iranian asylum seeker to Greece does
F not infringe article 3 of the ECHR, precludes a finding of an infringement of articles 1, 18 and 47 of the Charter in a case like the main proceedings.

140 As I have already explained, in its judgment of 21 January 2011 in *MSS v Belgium and Greece* 53 EHRR 28, ie after the order for reference was lodged, the European Court of Human Rights further developed its case law and considered the transfer of an asylum seeker from Belgium to Greece
G pursuant to Regulation No 343/2003 to be a violation by Belgium of article 3 of the ECHR and of article 13 in conjunction with article 3 of the ECHR.

141 In the light of this development in the European Court of Human Rights' case law, it would appear that the referring court is no longer required primarily to address the question under what circumstances the transfer of asylum seekers to Greece could, despite the European Court of
H Human Rights' decision in *KRS v United Kingdom*, lead to a finding of a violation of that asylum seeker's rights as enshrined in the Charter, but rather the question whether, having regard to the European Court of Human Rights' judgment in *MSS v Belgium and Greece*, a transfer of asylum seekers to Greece can actually still be found to be compatible with the Charter.

142 Against this background, the fifth question must therefore be construed as meaning that the court is being asked to clarify the relationship between articles 3 and 13 of the ECHR and the relevant provisions of the Charter[23] and the way in which the case law of the European Court of Human Rights on the (in)compatibility with the ECHR of transfers of asylum seekers to Greece affects the judicial review of the compatibility of such transfers with the Charter.

143 In answering these questions, regard must be had to article 52(3) of the Charter. Under that provision, the rights contained in the Charter which correspond to rights guaranteed by the ECHR have the same meaning and scope as the corresponding rights laid down by the ECHR. It is also expressly provided in article 52(3) of the Charter that that provision does not prevent European Union law providing more extensive protection.

144 In the Explanations relating to article 52(3) of the Charter it is stressed that that provision is intended to ensure the necessary consistency between the Charter and the ECHR. According to the Explanations, that reference should be construed not only as a reference to the text of the ECHR and the Protocols to it, but also to the clarification in the case law of the European Court of Human Rights of the meaning and the scope of the guaranteed rights. This does not, however, adversely affect the autonomy of European Union law and of that of the Court of Justice.

145 Under article 52(3) of the Charter, it must therefore be ensured that the protection guaranteed by the Charter in the areas in which the provisions of the Charter overlap with the guarantees under the ECHR is no less than the protection granted by the ECHR. Because the protection granted by the ECHR is constantly developing in the light of its interpretation by the European Court of Human Rights[24], the reference to the ECHR contained in article 52(3) of the Charter is to be construed as an essentially dynamic reference which, in principle, covers the case law of the European Court of Human Rights[25].

146 It should be borne in mind in this connection that the judgments of the European Court of Human Rights essentially always constitute case-specific judicial decisions and not the rules of the ECHR themselves, and it would therefore be wrong to regard the case law of the European Court of Human Rights as a source of interpretation with full validity in connection with the application of the Charter: see also the opinion of Advocate General Poiares Maduro of 9 September 2008 in *Elgafaji v Staatssecretaris van Justitie* (Case C-465/07) [2009] 1 WLR 2100; [2009] ECR I-921, para 23. This finding, admittedly, may not hide the fact that particular significance and high importance are to be attached to the case law of the European Court of Human Rights in connection with the interpretation of the Charter, with the result that it must be taken into consideration in interpreting the Charter[26].

147 This view is confirmed in the case law of the Court of Justice, which systematically takes into consideration the case law of the European Court of Human Rights on the relevant provisions of the ECHR in interpreting the provisions of the Charter[27].

148 In the light of the foregoing, the fifth question must be answered to the effect that under article 52(3) of the Charter it must be ensured that the protection guaranteed by the Charter in the areas in which the provisions of the Charter overlap with the provisions of the ECHR is no less than the

protection granted by the ECHR. Because the extent and scope of the protection granted by the ECHR has been clarified in the case law of the European Court of Human Rights, particular significance and high importance are to be attached to that case law in connection with the interpretation of the relevant provisions of the Charter by the Court of Justice.

D—Sixth question: Judicial review of compliance with the Geneva Convention and the ECHR in the member state primarily responsible under Regulation No 343/2003

149 With its sixth question, the referring court wishes to know whether a national law under which, in their review of the application of Regulation No 343/2003, the courts must proceed from the conclusive presumption that the state primarily responsible for examining the asylum application is a safe country in which asylum seekers are not exposed to the risk of expulsion to a persecuting state, which is incompatible with the Geneva Convention or with the ECHR, is compatible with article 47 of the Charter.

150 In order to answer this question, I will first examine the relationship between the rights of asylum seekers under article 47 of the Charter and risk of expulsion to a persecuting state, which is incompatible with the Geneva Convention and with the ECHR and which may arise in the event of a transfer of asylum seekers to the member state which is primarily responsible. On the basis of those observations I will then answer the sixth question asked by the referring court.

1. Article 47(1) of the Charter and the risk of infringement of the Convention on the Status of Refugees or of the ECHR following the transfer of an asylum seeker pursuant to Regulation No 343/2003

151 Under article 47(1) of the Charter, everyone whose rights and freedoms guaranteed by the law of the European Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article.

152 The basic condition for the applicability of article 47 of the Charter is therefore that rights and freedoms guaranteed by the law of the European Union are violated. Against this background, an infringement of the Geneva Convention or the ECHR can establish a right to an effective remedy under article 47(1) of the Charter only if that infringement is also to be regarded as a violation of rights and freedoms guaranteed by the law of the European Union.

153 Even though an infringement of the Geneva Convention or the ECHR in connection with the transfer of an asylum seeker to a member state in which there is a serious risk of his expulsion to a persecuting state must be distinguished strictly, de jure, from any associated infringement of European Union law, there is, as a rule, a de facto parallel in such a case between the infringement of the Geneva Convention or the ECHR and the infringement of European Union law.

154 In assessing whether the transfer of an asylum seeker to a member state in which there is a serious risk of his expulsion to another state in contravention of the Geneva Convention is consistent with European Union law, regard must be had to article 18 of the Charter, under which the right to

asylum is to be guaranteed with due respect for the rules of the Geneva Convention: see point 114 et seq of this opinion. By virtue to this express reference to the Geneva Convention, article 18 of the Charter grants refugees who have lodged an asylum application protection against transfers which are incompatible with the Geneva Convention[28]. Accordingly, the transfer of a refugee to the member state primarily responsible for his asylum application is incompatible with the Charter where there is a serious risk in that member state of direct or indirect expulsion to a persecuting state, which is incompatible with the Geneva Convention.

155 In assessing whether the transfer of an asylum seeker to a member state in which there is a serious risk of his expulsion to a third country in contravention of the ECHR is consistent with European Union law, regard must be had to the principle laid down in article 52(3) of the Charter, according to which the protection of the rights enshrined in the Charter may be no less than the guarantees under the ECHR: see point 143 et seq of this opinion.

156 In this connection, the European Court of Human Rights clarified the guarantees under the ECHR regarding the transfer of asylum seekers between member states most recently in its judgment in *MSS v Belgium and Greece* 53 EHRR 28. It held that the removal of an asylum seeker to an intermediary country, which is also a contracting party, leaves the responsibility of the transferring state intact, and that state is required, in accordance with article 3 of the ECHR, not to deport a person where substantial grounds have been shown for believing that the person in question, if transferred to the intermediary country, would face a real risk of being exposed to a transfer to another state contrary to article 3: *MSS v Belgium and Greece*, para 342.

157 Having regard to article 52(3) of the Charter, in the event that the transfer of an asylum seeker to the member state primarily responsible under Regulation No 343/2003 were to infringe article 3 of the ECHR because of the risk of indirect refoulement, there would generally also be an infringement of the Charter. In this connection, there may be, in particular, a violation of the asylum seeker's fundamental rights as enshrined in article 1, article 4 and article 19(2) of the Charter[29].

158 In the light of the foregoing, it must be stated, in summary, that the transfer of an asylum seeker to the member state primarily responsible under Regulation No 343/2003 is, as a rule, incompatible with European Union law where the asylum seeker is exposed in that member state to the serious risk of expulsion to a persecuting state which is incompatible with the Geneva Convention or with the ECHR. If the transfer of the asylum seeker infringes European Union law, article 47 of the Charter is applicable.

2. Incompatibility with article 47 of the Charter of the conclusive legal presumption that the asylum seeker will not be exposed, in the member state which is primarily responsible, to the risk of expulsion to another state, which is incompatible with the Geneva Convention and with the ECHR

159 Under article 47(1) of the Charter, everyone whose rights and freedoms guaranteed by the law of the European Union are violated has the right to an effective remedy before a tribunal in order to review that violation. Because that remedy is intended to clarify whether rights or

A freedoms actually guaranteed by the law of the European Union are violated, this right to an effective remedy arises from the time that an arguable complaint relating to the infringement is made[30].

160 The specific procedural form of the effective remedy within the meaning of article 47 of the Charter is largely left to the member states. However, this margin of discretion enjoyed by the member states is limited by the requirement that the effectiveness of the remedy must always be guaranteed. It must also be borne in mind in this connection that, under article 52(1) of the Charter, any limitation on the exercise of the right to an effective remedy must be provided for by law[31] and respect the essence of that right and the principle of proportionality.

161 The minimum content of the right to an effective remedy includes the requirements that the remedy to be granted to the beneficiary must satisfy the principle of effectiveness[32]. According to that principle, the realisation of the rights conferred by European Union law may not be rendered practically impossible or excessively difficult: see the case law cited in point 134 of this opinion.

162 In my view, it is immediately evident from these comments on the essence and the minimum content of the right to an effective remedy under article 47 of the Charter that a national law under which, in their review of the transfer of an asylum seeker to the member state primarily responsible under Regulation No 343/2003, the courts must proceed from the conclusive presumption that that member state will not expel the asylum seeker to another state in contravention of the ECHR or the Geneva Convention is incompatible with article 47 of the Charter.

163 The crucial factor in this connection is that such a presumption renders excessively difficult or even precludes de facto the judicial review of the risk of chain deportation to a persecuting state, which is incompatible with the Charter. It would logically be difficult to understand if a national court rejected the risk of chain deportation to a persecuting state from the perspective of the ECHR and the Geneva Convention, but accepted the coextensive risk of chain deportation to a persecuting state from the perspective of the Charter. For that reason, the conclusive presumption at issue, under which the member state which is primarily responsible will not expel the asylum seeker to a persecuting state in contravention of the ECHR and the Geneva Convention, is incompatible with article 47 of the Charter.

164 In the light of the foregoing, the sixth question must be answered to the effect that a national law under which, in examining whether an asylum seeker may be lawfully transferred to another member state pursuant to Regulation No 343/2003, the courts must proceed from the conclusive presumption that that member state is a safe country in which asylum seekers are not exposed to the risk of expulsion to a persecuting state, which is contrary to the Geneva Convention or with the ECHR, is incompatible with article 47 of the Charter.

E—Seventh question

165 By its seventh question, the referring court asks the Court of Justice to clarify the content and scope of Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the

232

United Kingdom, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union. It essentially asks whether, having regard to that Protocol, the provisions of the Charter which are relevant to the present case can take full effect in the legal order of the United Kingdom.

166 With this question, the referring court thus wishes to ascertain whether, and if so to what extent, Protocol No 30 can be regarded as an "opt-out" from the Charter for the United Kingdom and the Republic of Poland.

167 In my view, the question whether Protocol No 30 is to be regarded as a general opt-out from the Charter for the United Kingdom and the Republic of Poland can be easily answered in the negative[33]. This conclusion is suggested by an analysis of the wording of Protocol No 30, having particular regard to its recitals.

168 Under article 1(1) of Protocol No 30, the Charter does not extend the ability of the Court of Justice, or any court or tribunal of Poland or of the United Kingdom, to find that the laws, regulations or administrative provisions, practices or action of Poland or of the United Kingdom are inconsistent with the fundamental rights, freedoms and principles that it reaffirms.

169 According to its wording, article 1(1) of Protocol No 30 therefore makes clear that the Charter does not have the effect of either shifting powers at the expense of the United Kingdom or Poland or of extending the field of application of European Union law beyond the powers of the European Union as established in the Treaties. Article 1(1) of Protocol No 30 thus merely reaffirms the normative content of article 51 of the Charter, which seeks to prevent precisely such an extension of European Union powers or of the field of application of European Union law: see point 71 et seq of this opinion; see also *Paul Craig, The Lisbon Treaty* (2010), p 239; I Pernice, "The Treaty of Lisbon and Fundamental Rights" in *Griller & Ziller (eds), The Lisbon Treaty. EU Constitutionalism without a Constitutional Treaty?* (2008), footnote 33, p 246 et seq. Article 1(1) of the Protocol does not therefore, in principle, call into question the validity of the Charter for the United Kingdom and for Poland[34].

170 This view is confirmed in the recitals in the Preamble to the Protocol, which confirms, in several places, the fundamental validity of the Charter in the Polish and the English legal orders: see House of Lords European Union Committee, "The Treaty of Lisbon: an impact assessment" (10th Report of Session 2007–2008) (HL 62-I), para 5.102. For example, the third recital states that under article 6EU the Charter is to be applied and interpreted by the courts of Poland and of the United Kingdom strictly in accordance with the explanations referred to in that article. Reference is made in the eighth and ninth recitals to the wish of Poland and the United Kingdom to clarify certain aspects of the application of the Charter and the application of the Charter in relation to the laws and administrative action of Poland and of the United Kingdom.

171 Whilst article 1(1) of Protocol No 30 does not call into question the validity of the Charter, but should merely be regarded as an express confirmation of the normative content of article 51 of the Charter, article 1(2) of Protocol No 30 appears to seek to clarify the validity of individual provisions of the Charter in the legal orders of the United

A Kingdom and Poland. Under article 1(2) of Protocol No 30, nothing in Title IV of the Charter creates justiciable rights applicable to Poland or the United Kingdom except in so far as such rights are provided for in their respective national laws.

172 Article 1(2) of Protocol No 30 relates to the social fundamental rights and principles grouped together under Title IV of the Charter: articles B 27–38. That title, entitled "Solidarity", is regarded as one of the most controversial areas in the evolution of the Charter. There was dispute not only over the fundamental question whether social rights and principles should be incorporated into the Charter, but also how many social rights should be included, how they should be organised in detail, what binding force they should have, and whether they should be classified as fundamental rights or as principles[35].

C 173 With the statement that Title IV of the Charter does not create justiciable rights applicable to Poland or the United Kingdom, article 1(2) of Protocol No 30 first reaffirms the principle, set out in article 51(1) of the Charter, that the Charter does not create justiciable rights as between private individuals. However, article 1(2) of Protocol No 30 also appears to rule out new European Union rights and entitlements being derived from D articles 27 to 38 of the Charter, on which those entitled could rely against the United Kingdom or against Poland[36].

174 Because the contested fundamental rights in the present case are not among the social fundamental rights and principles set out in Title IV of the Charter, however, there is no need to examine in any greater detail here the question of the precise validity and scope of article 1(2) of Protocol No 30. It is sufficient to refer to the tenth recital in the Preamble to Protocol No 30, E according to which references in that Protocol to the operation of specific provisions of the Charter are strictly without prejudice to the operation of other provisions of the Charter.

175 Article 2 of Protocol No 30 provides, lastly, that where a provision of the Charter refers to national laws and practices, it only applies to Poland or the United Kingdom to the extent that the rights or principles that it F contains are recognised in the law or practices of Poland or of the United Kingdom.

176 In the light of the above-mentioned recitals, it is not possible to infer from article 2 of Protocol No 30 a general opt-out from the Charter of Fundamental Rights for the United Kingdom and the Republic of Poland. Moreover, article 2 of Protocol No 30 applies solely to provisions of the G Charter which make reference to national laws and practices[37]. That is not the case with the provisions of the Charter which are relevant in the present case.

177 In the light of the foregoing, the seventh question must be answered to the effect that the interpretation of Protocol No 30 has not produced any findings which could call into question the validity for the United Kingdom of the provisions of the Charter which are relevant in the present case.

H

VII—Conclusion

178 In the light of the above considerations, I propose that the court answer the questions asked by the Court of Appeal (England and Wales) as follows:

(1) A decision made by a member state under article 3(2) of Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the member state responsible for examining an asylum application lodged in one of the member states by a third country national whether to examine a claim for asylum which is not its responsibility under the criteria set out in Chapter III of the Regulation constitutes a measure implementing European Union law for the purposes of article 51(1) of the Charter.

(2) A member state in which an asylum application has been lodged is obliged to exercise its right to examine that asylum application under article 3(2) of Regulation No 343/2003 where transfer to the member state primarily responsible under article 3(1) in conjunction with the provisions contained in Chapter III of Regulation No 343/2003 would expose the asylum seeker to a serious risk of violation of his fundamental rights as enshrined in the Charter. Serious risks of infringements of individual provisions of Council Directive 2003/9/EC of 27 January 2003 laying down minimum standards for the reception of asylum seekers, Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted and Council Directive 2005/85/EC of 1 December 2005 on minimum standards on procedures in member states for granting and withdrawing refugee status in the member state primarily responsible which do not also constitute a violation of the fundamental rights of the asylum seeker to be transferred are not sufficient, on the other hand, to create an obligation on the part of the transferring member state to exercise the right to assume responsibility for the examination itself under article 3(2) of Regulation No 343/2003.

(3) The obligation to interpret Regulation No 343/2003 in a manner consistent with fundamental rights precludes the operation of a conclusive presumption according to which the member state primarily responsible for examining an asylum application will observe the asylum seeker's fundamental rights under European Union law and all the minimum standards laid down in Directives 2003/9, 2004/83 and 2005/85. The member states are not barred, on the other hand, from proceeding from the rebuttable presumption, in applying Regulation No 343/2003, that the asylum seeker's human rights and fundamental rights will be observed in the member state primarily responsible for his asylum application.

(4) Under article 52(3) of the Charter it must be ensured that the protection guaranteed by the Charter in the areas in which the provisions of the Charter overlap with the provisions of the ECHR is no less than the protection granted by the ECHR. Because the extent and scope of the protection granted by the ECHR has been clarified in the case law of the European Court of Human Rights, particular significance and high importance are to be attached to that case law in connection with the interpretation of the relevant provisions of the Charter by the Court of Justice.

(5) A national law under which, in examining whether an asylum seeker may be lawfully transferred to another member state pursuant to Regulation No 343/2003, the courts must proceed from the conclusive presumption that that member state is a safe country in which asylum seekers are not exposed

A to the risk of expulsion to a persecuting state, which is contrary to the Geneva Convention or with the ECHR, is incompatible with article 47 of the Charter.

(6) The interpretation of Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom has not produced any findings which could call into
B question the validity for the United Kingdom of the provisions of the Charter which are relevant in the present case.

Notes

1. In addition to the Regulation and the Directives mentioned here, there are many other pieces of secondary legislation which relate to the creation of a common asylum system, the policy of legal immigration, and the fight against illegal immigration,
C such as Parliament and Council Regulation (EU) No 439/2010 of 19 May 2010 establishing an European Asylum Support Office (OJ 2010 L132, p 11) and Parliament and Council Directive 2008/115/EC of 16 December 2008 on common standards and procedures in member states for returning illegally staying third country nationals (OJ 2008 L348, p 98).

2. The United Kingdom Government has answered the other questions in the event that, contrary to its proposal, the court were to conclude that the decision on
D the exercise of the right to assume responsibility for the examination under article 3(2) of Regulation No 343/2003 does fall within the scope of European Union law.

3. On the basis of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the state responsible for examining a request for asylum lodged in a member state or in Switzerland (OJ 2008 L53, p 5), the Swiss Confederation participates in the European Union's system for establishing the states responsible for asylum
E applications. Under article 5(2) of that Agreement, the Swiss Confederation has the right to submit statements of case or written observations to the Court of Justice in cases where a court in a member state has applied to the Court of Justice for a preliminary ruling concerning the interpretation of Regulation No 343/2003.

4. In the main proceedings, the referring court considers that it must address this question because the Secretary of State had argued that, in exercising their discretion under article 3(2) of Regulation No 343/2003, the member states are not required to
F take account of European Union fundamental rights, because the exercise of that discretion does not fall within the scope of European Union law.

5. See also the Explanations relating to the Charter of Fundamental Rights (OJ 2007 C303, p 32).

6. Under article 52(7) of the Charter, the Explanations, drawn up as a way of providing guidance in the interpretation of the Charter, are to be given due regard by the courts of the European Union and of the member states. The importance of the
G Explanations for the interpretation of the individual provisions of the Charter is also expressly confirmed in the third sub-paragraph of article 6(1)EU.

7. Under article 3(2) of Regulation No 343/2003, the member state which decides voluntarily to examine the application for asylum becomes the member state responsible within the meaning of that Regulation and assumes the obligations associated with that responsibility.

8. Under article 1 et seq of Protocol (No 5) on the position of Denmark, annexed
H to the Treaty on European Union and to the Treaty establishing the European Community, Denmark did not take part in the adoption of those Directives and those Directives are not therefore binding on or applicable in Denmark: see recital (21) in the Preamble to Directive 2003/9, recital (40) in the Preamble to Directive 2004/83, and recital (34) in the Preamble to Directive 2005/85. Whilst under article 3 of Protocol (No 4) on the position of the United Kingdom and Ireland, annexed to the

Treaty on European Union and to the Treaty establishing the European Community, Ireland took part in the adoption of Directives 2004/83 and 2005/85 (see recitals (39) and (33) in the Preambles to those Directives), it did not take part in the adoption of Directive 2003/9 pursuant to article 1 of that Protocol: see recital (20) in the Preamble to that Directive. The United Kingdom took part in the adoption of the three Directives pursuant to article 3 of that Protocol: see recital (19) in the Preamble to Directive 2003/9, recital (38) in the Preamble to Directive 2004/83, and recital (32) in the Preamble to Directive 2005/85.

9. See also, in this connection, *Abdulla v Bundesrepublik Deutschland* (Joined Cases C-175/08, C-176/08, C-178/08 and C-179/08) [2011] QB 46; [2010] ECR I-1493, para 51 et seq, and *Federal Republic of Germany v B* (Joined Cases C-57/09 and C-101/09) [2012] 1 WLR 1076, para 77 et seq, in which the court held, in connection with the interpretation of Directive 2004/83, first that the provisions of the Directive for determining who qualifies for refugee status and the content thereof were adopted to guide the competent authorities of the member states in the application of the Geneva Convention on the basis of common concepts and criteria and, second, that those provisions must be interpreted in a manner which respects the fundamental rights and the principles recognised in particular by the Charter. See also, in this connection, *Bolbol v Bevándorlási és Állampolgársági Hivatal* (Case C-31/09) [2010] ECR I-5539; [2012] All ER (EC) 469, para 38.

10. Under article 1 et seq of Protocol (No 5) on the position of Denmark, annexed to the Treaty on European Union and to the Treaty establishing the European Community, Denmark did not take part in the adoption of Regulation No 343/2003 and was not therefore initially bound by it nor subject to its application. The Dublin Convention thus remained in force between Denmark and the member states: see recital 1(8) et seq in the Preamble to Regulation No 343/2003. With the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the state responsible for examining a request for asylum lodged in Denmark or any other member state of the European Union and Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention (OJ 2006 L66, p 38), the scope of Regulation No 343/2003 was extended to the relations between the Community and Denmark. Ireland and the United Kingdom took part in the adoption and application of that Regulation in accordance with article 3 of Protocol (No 4) on the position of the United Kingdom and Ireland, annexed to the Treaty on European Union and to the Treaty establishing the European Community: see recital (17) in the Preamble to Regulation No 343/2003. It should also be borne in mind that some non-EU member states have participated under international agreements in the European Union system for determining the state responsible for asylum applications, such as the Swiss Confederation; see note 3 to this opinion.

11. Against this background, reference is also made in the recitals in the Preamble to Regulation No 343/2003 to the conclusion of the Tampere European Council, according to which the Common European Asylum System to be developed is to be based on the full and inclusive application of the Geneva Convention: see recital (2) in the Preamble to Regulation No 343/2003. It is also stressed that the member states are bound by the instruments of international law to which they are party with respect to the treatment of persons falling within the scope of that Regulation (see recital (12) in the Preamble to Regulation No 343/2003) and that the Regulation observes the fundamental rights and principles which are acknowledged in the Charter: see recital (15) in the Preamble to Regulation No 343/2003.

12. On the other hand, the Commission's Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the member state responsible for examining an application for international protection lodged in one of the member states by a third country national or a stateless person (COM(2008) 820 final), by which Regulation No 343/2003 was to be recast, provides for a mechanism for the temporary

A suspension of transfers of asylum seekers to member states faced with a particularly urgent situation which places an exceptionally heavy burden on their reception capacities, asylum systems or infrastructures: article 31. According to the Commission's Explanatory Memorandum, the proposal is aimed at addressing situations of particular pressure on member states' reception capacities and asylum systems.

13. The question whether, and if so in what circumstances, article 1 of the Charter
B can apply autonomously, in addition to article 4 of the Charter, does not need to be examined in any greater depth for the purposes of the present case. It should be pointed out, however, that, according to the prevailing opinion in German legal literature, an examination of article 4 of the Charter should be carried out first. If interference in the protection afforded by this specific fundamental right were to be taken to exist, this specific fundamental right would prevail and rule out article 1 of the Charter as an isolated or supplementary basis for assessment: see *Hans D Jarass,*
C *Charta der Grundrechte der Europäischen Union* (2010), article 1, para 4; D Borowsky, in *J Meyer (ed), Charta der Grundrechte der Europäischen Union*, 3rd ed, article 1, para 33; W Höfling, in *Tettinger & Stern (eds), Kölner Gemeinschaftskommentar zur Europäischen Grundrechte-Charta* (2006), article 1, para 18.

14. The question whether, and if so in what circumstances, article 1 and/or article 4 of the Charter can apply autonomously, in addition to article 19(2) of the
D Charter, does not need to be examined in any greater depth for the purposes of the present case. It should be pointed out, however, that, according to the prevailing opinion in German legal literature, in the event of an overlap with article 1 and/or article 4 of the Charter, article 19(2) of the Charter prevails as the specific provision for the examination: see *Hans D Jarass, Charta der Grundrechte der Europäischen Union*, article 19, para 4.

15. With the finding that the right to asylum is guaranteed with due respect for the
E rules of the EU Treaty and the FEU Treaty, reference is made, inter alia, to Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the EU Treaty and the FEU Treaty. Because, however, under article 3 of the Protocol on the position of the United Kingdom and Ireland, annexed to the Treaty on European Union and to the Treaty establishing the European Community, the United Kingdom took part in Directives 2003/9, 2004/85 and 2005/85 and in Regulation No 343/2003, the question of the
F effective force of article 18 of the Charter vis-à-vis the United Kingdom does not arise in the main proceedings.

16. Because the prohibition on return under article 33 of the Geneva Convention applies to refugees, the scope of the protection afforded by article 18 of the Charter in this regard is influenced by the notion of "refugee" in the Geneva Convention: see *Hans D Jarass, Charta der Grundrechte der Europäischen Union*, article 18, para 5. In the context of the prohibition on return under article 33 of the Geneva
G Convention, the notion of "refugee" covers not only those who have already been recognised as refugees, but also those who fulfil the conditions for recognition as a refugee. See Sir Elihu Lauterpacht and Daniel Bethlehem, "The scope and content of the principle of non-refoulement: opinion", in *Feller, Türk & Nicholson (eds), Refugee Protection in International Law* (2003), pp 87, 116 et seq.

17. See also, in this connection, Koen Lenaerts, "The Contribution of the European Court of Justice to the Area of Freedom, Security and Justice" (2010)
H ICLQ 255, 298, who concludes, after a rigorous analysis of the court's most recent case law, that in its rulings the court is concerned with respecting the fundamental rights dimension of the European asylum system.

18. See also *Abdulla v Bundesrepublik Deutschland* [2011] QB 46, para 54, and *Bolbol v Bevándorlási és Állampolgársági Hivatal* (Case C-31/09) [2010] ECR I-5539, [2012] All ER (EC) 469, para 38, with regard to the similarly worded recital

(10) in the Preamble to Directive 2004/83 and the resulting duty to interpret the provisions of the Directive in a manner consistent with fundamental rights. A

19. According to settled case law, in interpreting a provision of European Union law it is necessary to consider not only its wording, but also the context in which it occurs and the objective pursued by the rules of which it is part: see *Migrationsverket v Petrosian* (Case C-19/08) [2009] ECR I-495, para 34.

20. With regard to the content and scope of Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom, see point 165 et seq of this opinion. B

21. For example, in its decision of 2 December 2008, *KRS v United Kingdom* 48 EHRR SE 129, the European Court of Human Rights held that it must be presumed that Greece would comply with the obligations under Directives 2005/85 and 2003/9.

22. See also, in this connection, Protocol (No 24) on asylum for nationals of member states of the European Union, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union. That Protocol points out, first of all, that given the level of protection of fundamental rights and freedoms by the member states of the European Union, member states are to be regarded as constituting safe countries of origin in respect of each other for all legal and practical purposes in relation to asylum matters. Against this background, the Protocol then states that any application for asylum made by a national of a member state may be taken into consideration or declared admissible for processing by another member state only under the very restrictive conditions set out in the Protocol. C D

23. Articles 3 and 13 of the ECHR have their counterpart in articles 4 and 47(1) of the Charter. In the Explanations relating to article 4 of the Charter, it is stated that the right in article 4 is the right guaranteed by article 3 of the ECHR, which has the same wording, with the result that, by virtue of article 52(3) of the Charter, it has the same meaning and the same scope as the ECHR. The Explanations relating to article 47(1) state that that provision is based on article 13 of the ECHR, but nevertheless grants more extensive protection, since it guarantees the right to an effective remedy before a court. E

24. The European Court of Human Rights has confirmed in consistent case law that the ECHR is to be construed as a "living instrument": see *Tyrer v United Kingdom* (1978) 2 EHRR 1, para 31 and *V v United Kingdom* (1999) 30 EHRR 121, para 72.

25. See also, in this connection, *Rengeling & Szczekalla, Grundrechte in der Europäischen Union* (2004), para 468, who point out that article 52(3) of the Charter brings a high degree of dynamism to the development of European Union fundamental rights. Kolja Naumann "Art 52 Abs 3 GrCh zwischen Kohärenz des europäischen Grundrechtsschutzes und Autonomie des Unionsrechts" (2008) EuR 424, points out that, without taking into consideration the case law of the European Court of Human Rights, it is not possible to state, in any case, the meaning and the scope of the rights under the ECHR, and that only a dynamic reference can prevent the case law of the Court of Justice and the case law of the European Court of Human Rights drifting apart. F G

26. See also, in this connection T Von Danwitz, article 52, in *Tettinger & Stern (eds), Europäische Grundrechtecharta* (2006), p 774, para 57 et seq, who stresses, on the one hand, that the Charter does not accord the European Court of Human Rights the exclusive power of interpretation of the relevant rights, but, on the other, concedes that the Court of Justice is bound by the interpretation by the European Court of Human Rights of the rights under the ECHR in so far as it may not fall short of the level of protection guaranteed by the European Court of Human Rights. See also Koen Lenaerts & E de Smijter "The Charter and the Role of the European Courts" (2001) Maastricht Journal of European and Comparative Law 90, 99, who appear to accept that the Court of Justice is required to respect and adopt the relevant case law of the European Court of Human Rights. H

27. See, most recently, *Volker & Markus Schecke GbR v Land Hessen (Bundesanstalt für Landwirtschaft und Ernähung, joint party)* (Joined Cases C-92/09 and C-93/09) [2012] All ER (EC) 127, para 43 et seq. See also *Elgafaji v Staatssecretaris van Justitie* (Case C-465/07) [2009] 1 WLR 2100, para 44, in which the court stressed as an obiter dictum that the interpretation given in that judgment of the relevant provisions of Directive 2004/83 was fully compatible with the ECHR, including the case law of the European Court of Human Rights relating to article 3 of the ECHR. In *McB v E* (Case C-400/10PPU) [2011] Fam 364, para 53, the court expressly found, with regard to article 7 of the Charter, that that provision must be given the same meaning and the same scope as article 8.1 of the ECHR, as interpreted by the case law of the European Court of Human Rights.

28. With regard to the reference to the Geneva Convention in article 18 of the Charter, see N Bernsdorff in *J Meyer (ed), Charta der Grundrechte der Europäischen Union*, 3rd ed, article 18, para 10; M Wollenschläger in *Heselhaus & Nowak (eds), Handbuch der Europäischen Grundrechte* (2006), § 16, para 32; G Jochum in *Tettinger & Stern (eds), Europäische Grundrechtecharta* (2006), article 18, p 453, para 6.

29. With regard to the question whether articles 1, 4 and 19(2) of the Charter are applicable autonomously of one another in the case of a transfer of an asylum seeker to a member state which is incompatible with those provisions, see, ante, notes 13, 14.

30. See *Hans D Jarass, Charta der Grundrechte der Europäischen Union*, article 47, para 11; S Alber in *J Meyer (ed), Charta der Grundrechte der Europäischen Union*, 3rd ed (2006), article 47, p 724, para 25; C Nowak in *Heselhaus & Nowak (eds), Handbuch der Europäischen Grundrechte*, § 51, para 32. See also the consistent case law of the European Court of Human Rights relating to article 13 of the ECHR, according to which the right to an effective remedy enshrined therein is applicable where there is an arguable complaint that the ECHR has been infringed. See *MSS v Belgium and Greece* 53 EHRR 28, para 288, and judgment of 26 October 2000 in *Kudla v Poland* (2000) 35 EHRR 198, para 157.

31. Because of this statutory limitation on restrictions of fundamental rights, limitations of the rights enshrined in the Charter must be provided for either by the European Union legislature or by the national legislature. Where the fundamental right is limited in the national legal order, however, that statutory limitation is to be given a broad interpretation with the result that—having particular regard to the different legal traditions of the member states—it can also include customary law or judge-made law: see *Hans D Jarass, Charta der Grundrechte der Europäischen Union*, article 52, para 28; D Borowsky in *J Meyer (ed), Charta der Grundrechte der Europäischen Union*, 3rd ed, article 52, para 20.

32. With regard to the role of the principle of effectiveness in the application of article 47 of the Charter, see S Alber in *J Meyer (ed), Charta der Grundrechte der Europäischen Union*, 3rd ed, article 47, para 34; Hans D Jarass, "Bedeutung der EU-Rechtsschutzgewährleistung für nationale und EU-Gerichte" (2011) NJW 1393, 1395. See also the consistent case law of the European Court of Human Rights relating to article 13 of the ECHR, according to which the right to an effective remedy enshrined therein must be construed as meaning that the remedy must be available to the beneficiary in practice as well as in law, allowing the competent national authority both to deal with the substance of the relevant Convention complaint and to grant appropriate relief: see *MSS v Belgium and Greece* 53 EHRR 28, para 290 et seq

33. See also House of Lords European Union Committee, "The Treaty of Lisbon: an impact assessment" (10th Report of Session 2007–2008) (HL 62-I), paras 5.87, 5.103. See also I Pernice, "The Treaty of Lisbon and Fundamental Rights" in *Griller & Ziller (eds), The Lisbon Treaty. EU Constitutionalism without a Constitutional Treaty?* (2008), pp 235, 245.

240

34. See also House of Lords European Union Committee, "The Treaty of Lisbon: an impact assessment" (10th Report of Session 2007–2008) (HL 62-I), para 5.103.a; Michael Dougan, "The Treaty of Lisbon 2007: winning minds, not hearts", (2008) 45(3) CMLR 617, 669. See also *Paul Craig, The Lisbon Treaty*, p 239, who rightly states, in this connection, that article 1(2) of Protocol No 30 would be meaningless if article 1(1) of the Protocol contained a general opt-out.

35. See E Riedel in *J Meyer, Charta der Grundrechte der Europäischen Union*, 3rd ed, before Title IV, para 7 et seq.

36. See House of Lords European Union Committee, , "The Treaty of Lisbon: an impact assessment" (10th Report of Session 2007–2008) (HL 62-I), para 5.103(b), in whose view article 1(2) of the Protocol prevents the court, in interpreting individual Title IV "rights", concluding that those "rights" represent legally enforceable rights which could be relied on against the United Kingdom.

37. See also Michael Dougan, "The Treaty of Lisbon 2007: winning minds, not hearts" 45(3) CMLR 617, 670; House of Lords European Union Committee, "The Treaty of Lisbon: an impact assessment" (10th Report of Session 2007–2008) (HL 62-I), para 5.103(c); I Pernice "The Treaty of Lisbon and Fundamental Rights" in *Griller & Ziller (eds), The Lisbon Treaty. EU Constitutionalism without a Constitutional Treaty?*, p 248 et seq.

22 September 2011. **ADVOCATE GENERAL V TRSTENJAK** delivered an opinion in Case C-493/10. It substantially reiterates in relation to the questions raised in that case his opinion in case C-411/10, ante paras 84–136, and is not included in this report.

21 December 2011. **THE COURT (Grand Chamber)** delivered the following judgment.

1 The two references for preliminary rulings concern the interpretation, first, of article 3(2) of Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the member state responsible for examining an asylum application lodged in one of the member states by a third country national (OJ 2003 L50, p 1) and, second, the fundamental rights of the European Union, including the rights set out in articles 1, 4, 18, 19(2) and 47 of the Charter of Fundamental Rights of the European Union (OJ 2010 C83, p 389) ("the Charter") and, third, Protocol (No 30) on the application of the Charter to Poland and to the United Kingdom (OJ 2010 C83, p 313) ("Protocol No 30").

2 The references have been made in proceedings between asylum seekers who were to be returned to Greece pursuant to Regulation No 343/2003 and, respectively, the United Kingdom and Irish authorities.

Legal context

International law

3 The Convention relating to the Status of Refugees, signed in Geneva on 28 July 1951 (Cmd 9171) ("the Geneva Convention"), entered into force on 22 April 1954. It was extended by the Protocol relating to the Status of Refugees of 31 January 1967, which entered into force on 4 October 1967 (Cmnd 3906) ("the 1967 Protocol").

4 All the member states are contracting parties to the Geneva Convention and the 1967 Protocol, as are the Republic of Iceland, the Kingdom of Norway, the Swiss Confederation and the Principality of

241

A Liechtenstein. The European Union is not a contracting party to the Geneva Convention or to the 1967 Protocol, but article 78FEU of the FEU Treaty and article 18 of the Charter provide that the right to asylum is to be guaranteed with due respect for the Geneva Convention.

5 Article 33(1) of the Geneva Convention, headed "Prohibition of expulsion or return ('refoulement')", provides:

B

> "No contracting state shall expel or return ('refouler') a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion."

The Common European Asylum System

C 6 In order to achieve the objective, laid down by the European Council meeting in Strasbourg on 8 and 9 December 1989, of the harmonisation of their asylum policies, the member states signed in Dublin, on 15 June 1990, the Convention determining the state responsible for examining applications for asylum lodged in one of the member states of the European Communities (OJ 1997 C254, p 1) ("the Dublin Convention"). The Dublin Convention entered into force on 1 September 1997 for the 12 original signatories, on
D 1 October 1997 for the Republic of Austria and the Kingdom of Sweden, and on 1 January 1998 for the Republic of Finland.

7 The conclusions of the European Council meeting in Tampere on 15 and 16 October 1999 envisaged, inter alia, the establishment of a Common European Asylum System, based on the full and inclusive application of the Geneva Convention, thus ensuring that nobody is sent back to a place where
E they again risk being persecuted, that is to say, maintaining the principle of non-refoulement.

8 The Amsterdam Treaty of 2 October 1997 introduced article 63EC into the EC Treaty, which conferred competence on the European Community to adopt the measures recommended by the European Council in Tampere. That treaty also annexed to the EC Treaty the Protocol (No 24) on asylum for nationals of member states of the European Union
F (OJ 2010 C83, p 305), according to which those states are to be regarded as constituting safe countries of origin in respect to each other for all legal and practical purposes in relation to asylum matters.

9 The adoption of article 63EC made it possible, inter alia, to replace between the member states, with the exception of the Kingdom of Denmark, the Dublin Convention by Regulation No 343/2003, which entered into
G force on 17 March 2003. It is also on that legal basis that the Directives applicable to the cases in the main proceedings were adopted, for the purpose of establishing the Common European Asylum System foreseen by the conclusions of the Tampere European Council.

10 Since entry into force of the Lisbon Treaty, the relevant provisions in asylum matters are article 78FEU of the FEU Treaty, which provides for the establishment of a Common European Asylum System, and article 80FEU,
H which reiterates the principle of solidarity and fair sharing of responsibility between the member states.

11 The European Union legislation of relevance to the present cases includes: (1) Regulation No 343/2003; (2) Council Directive 2003/9/EC of 27 January 2003 laying down minimum standards for the reception of

asylum seekers (OJ 2003 L31, p 18); (3) Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted (OJ 2004 L304, p 12, and corrigendum, OJ 2005 L204, p 24); (4) Council Directive 2005/85/EC of 1 December 2005 on minimum standards on procedures in member states for granting and withdrawing refugee status (OJ 2005 L326, p 13, and corrigendum, OJ 2006 L236, p 36).

12 It is also appropriate to mention Council Directive 2001/55/EC of 20 July 2001 on minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between member states in receiving such persons and bearing the consequences thereof (OJ 2001 L212, p 12). As is apparent from recital (20) in the Preamble to that Directive, one of its objectives is to provide for a solidarity mechanism intended to contribute to the attainment of a balance of effort between member states in receiving and bearing the consequences of receiving displaced persons in the event of a mass influx.

13 The recording of the fingerprint data of foreign nationals illegally crossing an external border of the European Union makes it possible to determine the member state responsible for an asylum application. Such recording is provided for by Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention (OJ 2000 L316, p 1).

14 Regulation No 343/2003 and Directives 2003/9, 2004/83 and 2005/85 refer, in their first recitals, to the fact that a common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom, security and justice open to those who, forced by circumstances, legitimately seek protection in the Community. They also refer, in their second recitals, to the conclusions of the Tampere European Council.

15 Each of those texts states that it respects the fundamental rights and observes the principles recognised, in particular, by the Charter. Among others, recital (15) in the Preamble to Regulation No 343/2003 states that it seeks to ensure full observance of the right to asylum guaranteed by article 18 of the Charter; recital (5) in the Preamble to Directive 2003/9 states that, in particular, that Directive seeks to ensure full respect for human dignity and to promote the application of articles 1 and 18 of the Charter; and recital (10) in the Preamble to Directive 2004/83 states that, in particular, that Directive seeks to ensure full respect for human dignity and the right to asylum of applicants for asylum and their accompanying family members.

16 Article 1 of Regulation No 343/2003 lays down the criteria and mechanisms for determining the member state responsible for examining an application for asylum lodged in one of the member states by a third country national.

17 Article 3(1)(2) of that Regulation provide:

> "1. Member states shall examine the application of any third country national who applies at the border or in their territory to any one of them

for asylum. The application shall be examined by a single member state, which shall be the one which the criteria set out in Chapter III indicate is responsible.

"2. By way of derogation from paragraph 1, each member state may examine an application for asylum lodged with it by a third country national, even if such examination is not its responsibility under the criteria laid down in this Regulation. In such an event, that member state shall become the member state responsible within the meaning of this Regulation and shall assume the obligations associated with that responsibility. Where appropriate, it shall inform the member state previously responsible, the member state conducting a procedure for determining the member state responsible or the member state which has been requested to take charge of or take back the applicant."

18 In order to determine which is "the member state responsible" for the purposes of article 3(1) of Regulation No 343/2003, Chapter III of that Regulation lists objective and hierarchical criteria relating to unaccompanied minors, family unity, the issue of a residence document or visa, irregular entry into or residence in a member state and applications made in an international transit area of an airport.

19 Article 13 of that Regulation provides that, where no member state can be designated according to the hierarchy of criteria, the default rule is that the first member state with which the application was lodged will be responsible for examining the asylum application.

20 According to article 17 of Regulation No 343/2003, where a member state with which an application for asylum has been lodged considers that another member state is responsible for examining the application, it may, as quickly as possible, call on the other member state to take charge of the applicant.

21 Article 18(7) of that Regulation provides that failure by the requested member state to act before the expiry of a two-month period, or within one month where urgency is pleaded, is to be tantamount to accepting the request, and entails the obligation, for that member state, to take charge of the person, including the provisions for proper arrangements for arrival.

22 Article 19 of Regulation No 343/2003 is worded as follows:

"1. Where the requested member state accepts that it should take charge of an applicant, the member state in which the application for asylum was lodged shall notify the applicant of the decision not to examine the application, and of the obligation to transfer the applicant to the responsible member state.

"2. The decision referred to in paragraph 1 shall set out the grounds on which it is based. It shall contain details of the time limit for carrying out the transfer and shall, if necessary, contain information on the place and date at which the applicant should appear, if he is travelling to the member state responsible by his own means. This decision may be subject to an appeal or a review. Appeal or review concerning this decision shall not suspend the implementation of the transfer unless the courts or competent bodies so decide on a case-by-case basis if national legislation allows for this . . .

"4. Where the transfer does not take place within the six months' time limit, responsibility shall lie with the member state in which the application for asylum was lodged. This time limit may be extended up to a maximum of one year if the transfer could not be carried out due to imprisonment of the asylum seeker or up to a maximum of 18 months if the asylum seeker absconds . . ." A

23 The United Kingdom participates in the application of each of the Regulations and the four Directives mentioned in paras 11–13 of the present judgment. Ireland, by contrast, participates in the application of the Regulations and of Directives 2004/83, 2005/85 and 2001/55, but not Directive 2003/9. B

24 The Kingdom of Denmark is bound by the Agreement which it concluded with the European Community extending to Denmark the provisions of Regulation 2725/2000, approved by Council Decision 2006/188/EC of 21 February 2006 (OJ 2006 L66, p 37). It is not bound by the Directives referred to in para 11 of the present judgment. C

25 The European Community has also concluded an Agreement with the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the state responsible for examining a request for asylum lodged in a member state or Iceland or Norway, approved by Council Decision 2001/258/EC of 15 March 2001 (OJ 2001 L93, p 38). D

26 The European Community has similarly concluded an Agreement with the Swiss Confederation concerning the criteria and mechanisms for establishing the state responsible for examining a request for asylum lodged in a member state or in Switzerland, approved by Council Decision 2008/147/EC of 28 January 2008 (OJ 2008 L53, p 3), and the Protocol with the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the state responsible for examining a request for asylum lodged in a member state or in Switzerland, approved by Council Decision 2009/487/EC of 24 October 2008 (OJ 2009 L161, p 6). E F

27 Directive 2003/9 lays down minimum standards for the reception of asylum seekers in member states. Those standards concern in particular the obligations concerning the information and documents which must be provided to asylum seekers, the decisions which may be adopted by the member states concerning residence and freedom of movement of asylum seekers within their territory, families, medical screening, schooling and education of minors, employment of asylum seekers and their access to vocational training, the general rules on material reception conditions and health care available to asylum applicants, the modalities for material reception conditions and the health care which must be granted to asylum applicants. G

28 Directive 2003/9 also provides for an obligation to control the level of reception conditions and the possibility of appealing with regard to the matters and decisions covered by it. In addition, it contains rules concerning the training of the authorities and the necessary resources in connection with the national provisions enacted to implement the Directive. H

29 Directive 2004/83 lays down minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted. Chapter II thereof contains several provisions explaining how to assess applications. Chapter III thereof lays down the conditions which must be satisfied in order to qualify for being a refugee. Chapter IV concerns refugee status. Chapters V and VI concern the conditions which must be satisfied in order to qualify for subsidiary protection and the status conferred thereby. Chapter VII contains various rules setting out the content of international protection. According to article 20(1) of Directive 2004/83, that Chapter is to be without prejudice to the rights laid down in the Geneva Convention.

30 Directive 2005/85 lays down the rights of asylum seekers and the procedures for examining applications.

31 Article 36(1) of Directive 2005/85, under the heading "The European safe third countries concept" states:

> "member states may provide that no, or no full, examination of the asylum application and of the safety of the applicant in his/her particular circumstances as described in Chapter II, shall take place in cases where a competent authority has established, on the basis of the facts, that the applicant for asylum is seeking to enter or has entered illegally into its territory from a safe third country according to paragraph 2."

32 The conditions laid down in article 36(2) include: ratification of and compliance with the provisions of the Geneva Convention; the existence of an asylum procedure prescribed by law; ratification of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and compliance with its provisions, including the standards relating to effective remedies.

33 Article 39 of Directive 2005/85 sets out the effective remedies that it must be possible to pursue before the courts of the member states. Article 39(1)(a)(iii) refers to decisions not to conduct an examination pursuant to article 36 of the Directive.

The actions in the main proceedings and the questions referred for a preliminary ruling

Case C-411/10

34 NS, the claimant in the main proceedings, is an Afghan national who came to the United Kingdom after travelling through, among other countries, Greece. He was arrested in Greece on 24 September 2008 but did not make an asylum application.

35 According to him, the Greek authorities detained him for four days and, on his release, gave him an order to leave Greece within 30 days. He claims that, when he tried to leave Greece, he was arrested by the police and was expelled to Turkey, where he was detained in appalling conditions for two months. He states that he escaped from his place of detention in Turkey and travelled from that state to the United Kingdom, where he arrived on 12 January 2009 and where, that same day, he lodged an asylum application.

246

36 On 1 April 2009, the Secretary of State for the Home Department made a request to the Hellenic Republic, pursuant to article 17 of Regulation No 343/2003, to take charge of the the claimant in order to examine his asylum application. The Hellenic Republic failed to respond to that request within the time limit stipulated by article 18(7) of the Regulation and was accordingly deemed, on 18 June 2009, pursuant to that provision, to have accepted responsibility for examining the the appellant's claim.

37 On 30 July 2009, the Secretary of State notified the claimant that directions had been given for his removal to Greece on 6 August 2009.

38 On 31 July 2009, the Secretary of State notified the claimant of a decision certifying that, under paragraph 5(4) of Schedule 3 to the Asylum and Immigration (Treatment of Claimants, etc) Act 2004, his claim that his removal to Greece would violate his rights under the ECHR was clearly unfounded, since Greece is on the "list of safe countries" in Part 2 of Schedule 3 to the 2004 Act.

39 The consequence of that certification decision was, in accordance with paragraph 5(4) of Schedule 3 to the 2004 Act, that the claimant did not have a right to lodge an immigration appeal in the United Kingdom, with suspensive effect, against the decision ordering his transfer to Greece, an appeal to which he would have been entitled in the absence of such a certification decision.

40 On 31 July 2009, the claimant requested the Secretary of State to accept responsibility for examining his asylum claim under article 3(2) of the Regulation, on the ground that there was a risk that his fundamental rights under European Union law, the Human Rights Convention and/or the Geneva Convention would be breached if he were returned to Greece. By letter of 4 August 2009, the Secretary of State maintained his decision to transfer the claimant to Greece and his decision certifying that the claim of the claimant based on the ECHR was clearly unfounded.

41 On 6 August 2009, the claimant issued proceedings seeking judicial review of the Secretary of State's decisions. As a result, the Secretary of State annulled the directions for his transfer. On 14 October 2009, the permission sought by the appellant for judicial review was granted.

42 The application was examined by the High Court of Justice (England and Wales), Queen's Bench Division (Administrative Court) from 24 to 26 February 2010. By judgment of 31 March 2010, Cranston J dismissed the application but granted the claimant leave to appeal to the Court of Appeal (England and Wales) (Civil Division).

43 The claimant appealed to that court on 21 April 2010.

44 It emerges from the order for reference, in which the Court of Appeal refers to the judgment of the High Court of Justice (England and Wales), Queen's Bench Division (Administrative Court), that: (1) asylum procedures in Greece are said to have serious shortcomings: applicants encounter numerous difficulties in carrying out the necessary formalities; they are not provided with sufficient information and assistance; their claims are not examined with due care; (2) the proportion of asylum applications which are granted is understood to be extremely low; (3) judicial remedies are stated to be inadequate and very difficult to access; (4) the conditions for reception of asylum seekers are considered to be inadequate: applicants are either detained in inadequate conditions or they live outside in destitution, without shelter or food.

A 45 The High Court of Justice (England and Wales), Queen's Bench Division (Administrative Court) considered that the risks of refoulement from Greece to Afghanistan and Turkey were not established in the case of persons returned under Regulation No 343/2003, but that view is contested by the claimant before the referring court.

46 Before the Court of Appeal (England and Wales) (Civil Division), B the Secretary of State accepted [2010] EWCA Civ 990 at [7] that "the fundamental rights set out in the Charter can be relied on as against the United Kingdom and ... that the judge erred in holding otherwise". According to the Secretary of State, the Charter simply restates rights which already form an integral part of European Union law and does not create any new rights. However, the Secretary of State contended that the High Court of Justice (England and Wales) Queen's Bench Division (Administrative C Court) was wrong to find that she was bound to take into account European Union fundamental rights when exercising her discretion under article 3(2) of the Regulation. According to the Secretary of State, that discretionary power does not fall within the scope of European Union law.

47 In the alternative, the Secretary of State contended that the obligation to observe European Union fundamental rights does not require D her to take into account the evidence that, if the appellant were returned to Greece, there would be a substantial risk that his fundamental rights under European Union law would be infringed. She maintained that the scheme of Regulation No 343/2003 entitles her to rely on the conclusive presumption that Greece (or any other member state) would comply with its obligations under European Union law.

48 Finally, the claimant contended before the referring court that the E protection conferred by the Charter is higher than and goes beyond that guaranteed by, inter alia, article 3 of the ECHR, which might lead to a different outcome in the present case.

49 At the hearing of 12 July 2010, the referring court decided that decisions on certain questions of European Union law were necessary for it to give judgment on the appeal.

F 50 In those circumstances, the Court of Appeal (England and Wales) (Civil Division) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

"(1) Does a decision made by a member state under article 3(2) of ... Regulation No 343/2003 whether to examine a claim for asylum which is not its responsibility under the criteria set out in Chapter III of the G Regulation fall within the scope of European Union law for the purposes of article 6EU and/or article 51 of the Charter ... ?

"If question 1 is answered in the affirmative:

"(2) Is the duty of a member state to observe European Union fundamental rights (including the rights set out in articles 1, 4, 18, 19(2) and 47 of the Charter) discharged where that state sends the asylum seeker to the member state which article 3(1) [of Regulation H No 343/2003] designates as the responsible state in accordance with the criteria set out in Chapter III of the Regulation ('the responsible state'), regardless of the situation in the responsible state?

"(3) In particular, does the obligation to observe European Union fundamental rights preclude the operation of a conclusive presumption

that the responsible state will observe (i) the claimant's fundamental rights under European Union law; and/ or (ii) the minimum standards imposed by Directives 2003/9 . . . , 2004/83 . . . and 2005/85 . . . ?

"(4) Alternatively, is a member state obliged by European Union law, and, if so, in what circumstances, to exercise the power under article 3(2) of the Regulation to examine and take responsibility for a claim, where transfer to the responsible state would expose the [asylum] claimant to a risk of violation of his fundamental rights, in particular the rights set out in articles 1, 4, 18, 19(2) and/or 47 of the Charter, and/or to a risk that the minimum standards set out in Directives [2003/9, 2004/83 and 2005/85] will not be applied to him?

"(5) Is the scope of the protection conferred on a person to whom Regulation [No 343/2003] applies by the general principles of European Union law, and, in particular, the rights set out in articles 1, 18 and 47 of the Charter wider than the protection conferred by article 3 of the ECHR?

"(6) Is it compatible with the rights set out in article 47 of the Charter for a provision of national law to require a court, for the purpose of determining whether a person may lawfully be removed to another member state pursuant to Regulation [No 343/2003], to treat that member state as a state from which the person will not be sent to another state in contravention of his rights pursuant to the ECHR or his rights pursuant to the [Geneva Convention] and [the 1967 Protocol]?

"(7) In so far as the preceding questions arise in respect of the obligations of the United Kingdom, are the answers to [the second to sixth questions] qualified in any respect so as to take account of Protocol No 30?"

Case C-493/10

51 This case concerns five appellants in the main proceedings, all unconnected with each other, originating from Afghanistan, Iran and Algeria. Each of them travelled via Greece and was arrested there for illegal entry. They then travelled to Ireland, where they claimed asylum. Three of the appellants in the main proceedings claimed asylum without disclosing that they had previously been in Greece, whilst the other two admitted they had previously been in Greece. The Eurodac system confirmed that all five appellants had previously entered Greece, but that none of them had claimed asylum there.

52 Each of the appellants in the main proceedings resists return to Greece. As is apparent from the order for reference, it has not been argued that the transfer of the appellants to Greece under Regulation No 343/2003 would violate article 3 of the ECHR because of a risk of refoulement, chain refoulement, ill-treatment or suspension of asylum claims. It is also not alleged that the transfer would breach another article of the ECHR. The appellants in the main proceedings argued that the procedures and conditions for asylum seekers in Greece are inadequate and that Ireland is therefore required to exercise its power under article 3(2) of Regulation No 343/2003 to accept responsibility for examining and deciding on their asylum claims.

A 53 In those circumstances, the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

"(1) Is the transferring member state under ... Regulation No 343/2003 obliged to assess the compliance of the receiving member state with article 18 of the Charter ..., ... Directives 2003/9/EC,
B 2004/83/EC and 2005/85/EC and Regulation (EC) No 343/2003?

"(2) If the answer is yes, and if the receiving member state is found not to be in compliance with one or more of those provisions, is the transferring member state obliged to accept responsibility for examining the application under article 3(2) of ... Regulation No 343/2003?"

C 54 Cases C-411/10 and C-493/10 were, by order of the President of the Court of 16 May 2011, joined for the purposes of the written and oral procedure and the judgment.

Consideration of the questions referred for a preliminary ruling

The first question in Case C-411/10

D 55 By its first question in Case C-411/10, the Court of Appeal (England and Wales) (Civil Division) asks, in essence, whether the decision adopted by a member state on the basis of article 3(2) of Regulation No 343/2003 to examine a claim for asylum which is not its responsibility under the criteria set out in Chapter III of that Regulation falls within the scope of European Union law for the purposes of article 6EU and/or article 51 of the Charter.

E Observations submitted to the court

56 NS, the Equality and Human Rights Commission, Amnesty International Ltd ("Amnesty") and the AIRE Centre, the United Nations High Commissioner for Refugees, the French, Netherlands, Austrian and Finnish Governments and the commission consider that a decision adopted on the basis of article 3(2) of Regulation No 343/2003 falls within the scope of European Union law.

F 57 NS points out, in that regard, that the exercise of the power provided for by that provision will not necessarily be more favourable to the applicant, which explains why, in its assessment of the Dublin system (COM (2007) 299 final), the commission proposed that exercise of the power provided for by article 3(2) of Regulation No 343/2003 should be subject to the consent of the asylum seeker.

G 58 According to Amnesty and the AIRE Centre and the French Government, in particular, the possibility provided for in article 3(2) of Regulation No 343/2003 is justified by the fact that the purpose of the Regulation is to protect fundamental rights and that it might be necessary to exercise the power provided for by that article.

59 The Finnish Government emphasises that Regulation No 343/2003 forms part of a set of rules establishing a system.

H 60 According to the commission, when a Regulation confers a discretionary power on a member state, it must exercise that power in accordance with European Union law: see *Wachauf v Federal Republic of Germany* (Case 5/88) [1989] ECR 2609; *Chakroun v Minister van Buitenlandse Zaken* (Case C-578/08) [2010] ECR I-1839 and *McB v E*

250

(Case C-400/10PPU) [2011] Fam 364. It points out that a decision adopted by a member state on the basis of article 3(2) of Regulation No 343/2003 has consequences for that member state, which will be bound by the procedural obligations of the European Union and by the Directives.

61 Ireland, the United Kingdom, the Belgian Government and the Italian Government, on the other hand, consider that such a decision under article 3(2) of the Regulation does not fall within the scope of European Union law. The arguments put forward are the clarity of the text, which provides for an option, the reference to a "sovereignty" clause or "discretionary clause" in the commission documents, the raison d'être of such a clause, that is humanitarian grounds, and, lastly, the logic of the system established by Regulation No 343/2003.

62 The United Kingdom emphasises that a sovereignty clause is not a derogation within the meaning of *Elliniki Radiophonia Tiléorassi AE v Dimotiki Etairia Pliroforissis* (Case C-260/89) [1991] ECR I-2925, para 43. It also points out that the fact that the exercise of that clause does not implement European Union law does not mean that member states are disregarding fundamental rights, since they are bound by the Geneva Convention and the ECHR. The Belgian Government, however, submits that carrying out the decision to transfer the asylum seeker implements Regulation No 343/2003 and therefore falls within the scope of article 6EU and the Charter.

63 The Czech Government takes the view that the decision by a member state falls within European Union law when that state exercises the sovereignty clause, but not when it does not exercise that power.

The court's reply

64 Article 51(1) of the Charter states that the provisions thereof are addressed to the member states only when they are implementing European Union law.

65 Scrutiny of article 3(2) of Regulation No 343/2003 shows that it grants member states a discretionary power which forms an integral part of the Common European Asylum System provided for by the FEU Treaty and developed by the European Union legislature.

66 As stated by the commission, that discretionary power must be exercised in accordance with the other provisions of that Regulation.

67 In addition, article 3(2) of Regulation No 343/2003 states that the derogation from the principle laid down in article 3(1) of that Regulation gives rise to the specific consequences provided for by that Regulation. Thus, a member state which decides to examine an asylum application itself becomes the member state responsible within the meaning of Regulation No 343/2003 and must, where appropriate, inform the other member state or member states concerned by the asylum application.

68 Those factors reinforce the interpretation according to which the discretionary power conferred on the member states by article 3(2) of Regulation No 343/2003 forms part of the mechanisms for determining the member state responsible for an asylum application provided for under that Regulation and, therefore, merely an element of the Common European Asylum System. Thus, a member state which exercises that discretionary

A power must be considered as implementing European Union law within the meaning of article 51(1) of the Charter.

69 The answer to the first question in Case C-411/10 is therefore that the decision by a member state on the basis of article 3(2) of Regulation No 343/2003 whether to examine an asylum application which is not its responsibility according to the criteria laid down in Chapter III of that
B Regulation, implements European Union law for the purposes of article 6EU and/or article 51 of the Charter.

The second to fourth questions and the sixth question in Case C-411/10 and the two questions in Case C-493/10

70 By the second question in Case C-411/10 and the first question in
C Case C-493/10, the referring courts ask, in essence, whether the member state which should transfer the asylum seeker to the member state which article 3(1) of Regulation No 343/2003 indicates as responsible is obliged to assess the compliance, by that member state, with the fundamental rights of the European Union, Directives 2003/9, 2004/83 and 2005/85 and with Regulation No 343/2003.

71 By the third question in Case C-411/10, the Court of Appeal
D (England and Wales) (Civil Division) asks, in essence, whether the obligation on the member state which should transfer the asylum seeker to observe fundamental rights precludes the operation of a conclusive presumption that the responsible state will observe the claimant's fundamental rights under European Union law and/or the minimum standards imposed by the above-mentioned Directives.

E 72 By the fourth question in Case C-411/10 and the second question in Case C-493/10, the referring courts ask, in essence, whether, where the member state responsible is found not to be in compliance with fundamental rights, the member state which should transfer the asylum seeker is obliged to accept responsibility for examining the asylum application under article 3(2) of Regulation 343/2003?

73 Finally, by its sixth question in Case C-411/10, the Court of Appeal
F (England and Wales) (Civil Division) asks, in essence, whether a provision of national law which requires a court, for the purpose of determining whether a person may lawfully be removed to another member state pursuant to Regulation No 343/2003, to treat that member state as a "safe country" is compatible with the rights set out in article 47 of the Charter.

74 Those questions should be considered together.

G 75 The Common European Asylum System is based on the full and inclusive application of the Geneva Convention and the guarantee that nobody will be sent back to a place where they again risk being persecuted. Article 18 of the Charter and article 78FEU provide that the rules of the Geneva Convention and the 1967 Protocol are to be respected: see *Abdulla v Bundesrepublik Deutschland* (Joined Cases C-175/08, C-176/08, C-178/08 and C-179/08) [2011] QB 46; [2010] ECR I-1493, para 53, and *Bolbol v*
H *Bevándorlási és Állampolgársági Hivatal* (Case C-31/09) [2010] ECR I-5539, para 38.

76 As stated in para 15 above, the various Regulations and Directives relevant to the cases in the main proceedings provide that they comply with the fundamental rights and principles recognised by the Charter.

252

77 According to settled case law, the member states must not only interpret their national law in a manner consistent with European Union law but also make sure they do not rely on an interpretation of an instrument of secondary legislation which would be in conflict with the fundamental rights protected by the European Union legal order or with the other general principles of European Union law: see, to that effect, *Criminal proceedings against Lindqvist* (Case C-101/01) [2004] QB 1014; [2004] ECR I-12971, para 87 and *Ordre des barreaux francophones et germanophone v Conseil des ministres (Conseil des Barreaux de l'Union européene intervening)* (Case C-305/05) [2007] ECR I-5305; [2007] All ER (EC) 953, para 28.

78 Consideration of the texts which constitute the Common European Asylum System shows that it was conceived in a context making it possible to assume that all the participating states, whether member states or third states, observe fundamental rights, including the rights based on the Geneva Convention and the 1967 Protocol, and on the ECHR, and that the member states can have confidence in each other in that regard.

79 It is precisely because of that principle of mutual confidence that the European Union legislature adopted Regulation No 343/2003 and the Conventions referred to in paras 24–26 of the present judgment in order to rationalise the treatment of asylum claims and to avoid blockages in the system as a result of the obligation on state authorities to examine multiple claims by the same applicant, and in order to increase legal certainty with regard to the determination of the state responsible for examining the asylum claim and thus to avoid forum shopping, it being the principal objective of all these measures to speed up the handling of claims in the interests both of asylum seekers and the participating member states.

80 In those circumstances, it must be assumed that the treatment of asylum seekers in all member states complies with the requirements of the Charter, the Geneva Convention and the ECHR.

81 It is not however inconceivable that that system may, in practice, experience major operational problems in a given member state, meaning that there is a substantial risk that asylum seekers may, when transferred to that member state, be treated in a manner incompatible with their fundamental rights.

82 Nevertheless, it cannot be concluded from the above that any infringement of a fundamental right by the member state responsible will affect the obligations of the other member states to comply with the provisions of Regulation No 343/2003.

83 At issue here is the raison d'être of the European Union and the creation of an area of freedom, security and justice and, in particular, the Common European Asylum System, based on mutual confidence and a presumption of compliance, by other member states, with European Union law and, in particular, fundamental rights.

84 In addition, it would not be compatible with the aims of Regulation No 343/2003 were the slightest infringement of Directives 2003/9, 2004/83 or 2005/85 to be sufficient to prevent the transfer of an asylum seeker to the member state primarily responsible. Regulation No 343/2003 aims—on the assumption that the fundamental rights of the asylum seeker are observed in the member state primarily responsible for examining the application—to establish, as is apparent inter alia from points 124 and 125 of the opinion in Case C-411/10, a clear and effective method for dealing with an asylum

A application. In order to achieve that objective, Regulation No 343/2003 provides that responsibility for examining an asylum application lodged in an European Union country rests with a single member state, which is determined on the basis of objective criteria.

85 If the mandatory consequence of any infringement of the individual provisions of Directives 2003/9, 2004/83 or 2005/85 by the member state responsible were that the member state in which the asylum application was
B lodged is precluded from transferring the applicant to the first mentioned state, that would add to the criteria for determining the member state responsible set out in Chapter III of Regulation No 343/2003 another exclusionary criterion according to which minor infringements of the above-mentioned Directives committed in a certain member state may exempt that member state from the obligations provided for under Regulation
C No 343/2003. Such a result would deprive those obligations of their substance and endanger the realisation of the objective of quickly designating the member state responsible for examining an asylum claim lodged in the European Union.

86 By contrast, if there are substantial grounds for believing that there are systemic flaws in the asylum procedure and reception conditions for asylum applicants in the member state responsible, resulting in inhuman or
D degrading treatment, within the meaning of article 4 of the Charter, of asylum seekers transferred to the territory of that member state, the transfer would be incompatible with that provision.

87 With regard to the situation in Greece, the parties who have submitted observations to the court are in agreement that that member state was, in 2010, the point of entry in the European Union of almost 90% of
E illegal immigrants, that influx resulting in a disproportionate burden being borne by it compared to other member states and the inability to cope with the situation in practice. The Hellenic Republic stated that the member states had not agreed to the commission's proposal that the application of Regulation No 343/2003 be suspended and that it be amended by mitigating the criterion of first entry.

F 88 In a situation similar to those at issue in the cases in the main proceedings, that is to say the transfer, in June 2009, of an asylum seeker to Greece, the member state responsible within the meaning of Regulation No 343/2003, the European Court of Human Rights held, inter alia, that the Kingdom of Belgium had infringed article 3 of the ECHR, first, by exposing the applicant to the risks arising from the deficiencies in the asylum procedure in Greece, since the Belgian authorities knew or ought to have
G known that he had no guarantee that his asylum application would be seriously examined by the Greek authorities and, second, by knowingly exposing him to conditions of detention and living conditions that amounted to degrading treatment: *MSS v Belgium and Greece* 53 EHRR 28, paras 358, 360 and 367.

89 The extent of the infringement of fundamental rights described in that judgment shows that there existed in Greece, at the time of the transfer
H of the applicant MSS, a systemic deficiency in the asylum procedure and in the reception conditions of asylum seekers.

90 In finding that the risks to which the applicant was exposed were proved, the European Court of Human Rights took into account the regular and unanimous reports of international non-governmental organisations

254

bearing witness to the practical difficulties in the implementation of the Common European Asylum System in Greece, the correspondence sent by the United Nations High Commissioner for Refugees to the Belgian minister responsible, and also the commission reports on the evaluation of the Dublin system and the proposals for recasting Regulation No 343/2003 in order to improve the efficiency of the system and the effective protection of fundamental rights: *MSS v Belgium and Greece*, paras 347–350.

91 Thus, and contrary to the submissions of the Belgian, Italian and Polish Governments, according to which the member states lack the instruments necessary to assess compliance with fundamental rights by the member state responsible and, therefore, the risks to which the asylum seeker would be exposed were he to be transferred to that member state, information such as that cited by the European Court of Human Rights enables the member states to assess the functioning of the asylum system in the member state responsible, making it possible to evaluate those risks.

92 The relevance of the reports and proposals for amendment of Regulation No 343/2003 emanating from the commission should be noted—these must be known to the member state which has to carry out the transfer, given its participation in the work of the Council of the European Union, which is one of the addressees of those documents.

93 In addition, article 80FEU provides that asylum policy and its implementation are to be governed by the principle of solidarity and fair sharing of responsibility, including its financial implications, between the member states. Directive 2001/55 is an example of that solidarity but, as was stated at the hearing, the solidarity mechanisms which it contains apply only to wholly exceptional situations falling within the scope of that Directive, that is to say, a mass influx of displaced persons.

94 It follows from the foregoing that in situations such as that at issue in the cases in the main proceedings, to ensure compliance by the European Union and its member states with their obligations concerning the protection of the fundamental rights of asylum seekers, the member states, including the national courts, may not transfer an asylum seeker to the "member state responsible" within the meaning of Regulation No 343/2003 where they cannot be unaware that systemic deficiencies in the asylum procedure and in the reception conditions of asylum seekers in that member state amount to substantial grounds for believing that the asylum seeker would face a real risk of being subjected to inhuman or degrading treatment within the meaning of article 4 of the Charter.

95 With regard to the question whether the member state which cannot carry out the transfer of the asylum seeker to the member state identified as "responsible" in accordance with Regulation No 343/2003 is obliged to examine the application itself, it should be recalled that Chapter III of that Regulation refers to a number of criteria and that, in accordance with article 5(1) of that Regulation, those criteria apply in the order in which they are set out in that Chapter.

96 Subject to the right itself to examine the application referred to in article 3(2) of Regulation No 343/2003, the finding that it is impossible to transfer an applicant to Greece, where that state is identified as the member state responsible in accordance with the criteria set out in Chapter III of that Regulation, entails that the member state which should carry out that

A transfer must continue to examine the criteria set out in that chapter in order to establish whether one of the following criteria enables another member state to be identified as responsible for the examination of the asylum application.

97 In accordance with article 13 of Regulation No 343/2003, where the member state responsible for examining the application for asylum cannot be designated on the basis of the criteria listed in that Regulation, the first B member state with which the application for asylum was lodged is to be responsible for examining it.

98 The member state in which the asylum seeker is present must, however, ensure that it does not worsen a situation where the fundamental rights of that applicant have been infringed by using a procedure for determining the member state responsible which takes an unreasonable C length of time. If necessary, that member state must itself examine the application in accordance with the procedure laid down in article 3(2) of Regulation No 343/2003.

99 It follows from all of the foregoing considerations that, as stated by the Advocate General in para 131 of her opinion, an application of Regulation No 343/2003 on the basis of the conclusive presumption that the asylum seeker's fundamental rights will be observed in the member state D primarily responsible for his application is incompatible with the duty of the member states to interpret and apply Regulation No 343/2003 in a manner consistent with fundamental rights.

100 In addition, as stated by S, were Regulation No 343/2003 to require a conclusive presumption of compliance with fundamental rights, it could itself be regarded as undermining the safeguards which are intended to E ensure compliance with fundamental rights by the European Union and its member states.

101 That would be the case, inter alia, with regard to a provision which laid down that certain states are "safe countries" with regard to compliance with fundamental rights, if that provision had to be interpreted as constituting a conclusive presumption, not admitting of any evidence to the contrary. F

102 In that regard, it should be pointed out that article 36 of Directive 2005/85, concerning the safe third country concept, provides, in paragraph 2(a)(c), that a third country can only be considered as a "safe third country" where not only has it ratified the Geneva Convention and the ECHR but it also observes the provisions thereof.

103 Such wording indicates that the mere ratification of Conventions by G a member state cannot result in the application of a conclusive presumption that that state observes those Conventions. The same principle is applicable both to member states and third countries.

104 In those circumstances, the presumption underlying the relevant legislation, stated in para 80 above, that asylum seekers will be treated in a way which complies with fundamental rights, must be regarded as rebuttable. H

105 In the light of those factors, the answer to the questions referred is that European Union law precludes the application of a conclusive presumption that the member state which article 3(1) of Regulation No 343/2003 indicates as responsible observes the fundamental rights of the European Union.

106 Article 4 of the Charter of Fundamental Rights of the European Union must be interpreted as meaning that the member states, including the national courts, may not transfer an asylum seeker to the "member state responsible" within the meaning of Regulation No 343/2003 where they cannot be unaware that systemic deficiencies in the asylum procedure and in the reception conditions of asylum seekers in that member state amount to substantial grounds for believing that the asylum seeker would face a real risk of being subjected to inhuman or degrading treatment within the meaning of that provision.

107 Subject to the right itself to examine the application referred to in article 3(2) of Regulation No 343/2003, the finding that it is impossible to transfer an applicant to another member state, where that state is identified as the member state responsible in accordance with the criteria set out in Chapter III of that Regulation, entails that the member state which should carry out that transfer must continue to examine the criteria set out in that chapter in order to establish whether one of the following criteria enables another member state to be identified as responsible for the examination of the asylum application.

108 The member state in which the asylum seeker is present must, however, ensure that it does not worsen a situation where the fundamental rights of that applicant have been infringed by using a procedure for determining the member state responsible which takes an unreasonable length of time. If necessary, the first mentioned member state must itself examine the application in accordance with the procedure laid down in article 3(2) of Regulation No 343/2003.

The fifth question in Case C-411/10

109 By its fifth question in Case C-411/10, the Court of Appeal (England and Wales) (Civil Division) asks, in essence, whether the extent of the protection conferred on a person to whom Regulation No 343/2003 applies by the general principles of European Union law, and, in particular, the rights set out in articles 1, concerning human dignity, 18, concerning the right to asylum, and 47, concerning the right to an effective remedy, of the Charter, is wider than the protection conferred by article 3 of the ECHR.

110 According to the commission, the answer to that question must make it possible to identify the provisions of the Charter the infringement of which by the member state responsible would result in the secondary responsibility of the member state which has to decide on the transfer.

111 Even if the Court of Appeal (England and Wales) (Civil Division) did not expressly provide reasons, in the order for reference, why it required an answer to the question in order to give judgment, a reading of that decision in fact suggests that that question can be accounted for by the decision of 2 December 2008 in *KRS v United Kingdom* 48 EHRR SE 129 in which the European Court of Human Rights held inadmissible an application claiming that article 3 and 13 of the ECHR would be infringed were the applicant to be transferred by the United Kingdom to Greece. Before the Court of Appeal (England and Wales) (Civil Division), a number of parties claimed that the protection of fundamental rights stemming from the Charter is wider than that conferred by the ECHR and that, taking the

A Charter into account, their request not to transfer the applicant in the main proceedings to Greece would have to be granted.

112 After the order for reference was made, the European Court of Human Rights reviewed its position in the light of new evidence and held, in *MSS v Belgium and Greece* 53 EHRR 28, not only that the Hellenic Republic had infringed article 3 of the ECHR owing to the applicant's detention and
B living conditions in Greece and also article 13 of the ECHR read in conjunction with the aforesaid article 3 on account of the deficiencies in the asylum procedure conducted in the applicant's case, but also that the Kingdom of Belgium had infringed article 3 of the ECHR by exposing the applicant to the risks linked to the deficiencies in the asylum procedure in Greece and to detention and living conditions in Greece which did not comply with that article.

C 113 As follows from para 106 above, a member state would infringe article 4 of the Charter if it transferred an asylum seeker to the member state responsible within the meaning of Regulation No 343/2003 in the circumstances described in para 94 of the present judgment.

114 Articles 1, 18 and 47 of the Charter do not lead to a different answer than that given to the second to fourth questions and to the sixth
D question in Case C-411/10 and to the two questions in Case C-493/10.

115 Consequently, the answer to the fifth question in Case C-411/10 is that articles 1, 18 and 47 of the Charter do not lead to a different answer than that given to the second to fourth questions and to the sixth question in Case C-411/10 and to the two questions in Case C-493/10.

The seventh question in Case C-411/10

E

116 By its seventh question in Case C-411/10, the Court of Appeal (England and Wales) (Civil Division) asks, in essence, whether, in so far as the preceding questions arise in respect of the obligations of the United Kingdom, the answers to the second to sixth questions should be qualified in any respect so as to take account of Protocol No 30.

117 As noted by the Equality and Human Rights Commission, that
F question arises because of the position taken by the Secretary of State before the High Court of Justice (England and Wales) (Administrative Court) that the provisions of the Charter do not apply in the United Kingdom.

118 Even if the Secretary of State no longer maintained that position before the Court of Appeal (England and Wales) (Civil Division), it must be noted that Protocol No 30 provides, in article 1(1), that the Charter is not to
G extend the ability of the Court of Justice or any court or tribunal of Poland or of the United Kingdom, to find that the laws, regulations or administrative provisions, practices or action of Poland or of the United Kingdom are inconsistent with the fundamental rights, freedoms and principles that it affirms.

119 According to the wording of that provision, as noted by the Advocate General in points 169 and 170 of her opinion in Case C-411/10,
H Protocol No 30 does not call into question the applicability of the Charter in the United Kingdom or in Poland, a position which is confirmed by the recitals in the Preamble to that Protocol. Thus, according to the third recital in the Preamble to Protocol No 30, article 6EU requires the Charter to be applied and interpreted by the courts of Poland and of the United Kingdom

strictly in accordance with the explanations referred to in that article. In addition, according to the sixth recital in the Preamble to that Protocol, the Charter reaffirms the rights, freedoms and principles recognised in the Union and makes those rights more visible, but does not create new rights or principles.

120 In those circumstances, article 1(1) of Protocol No 30 explains article 51 of the Charter with regard to the scope thereof and does not intend to exempt the Republic of Poland or the United Kingdom from the obligation to comply with the provisions of the Charter or to prevent a court of one of those member states from ensuring compliance with those provisions.

121 Since the rights referred to in the cases in the main proceedings do not form part of Title IV of the Charter, there is no need to rule on the interpretation of article 1(2) of Protocol No 30.

122 The answer to the seventh question in Case C-411/10 is therefore that, in so far as the preceding questions arise in respect of the obligations of the United Kingdom, the answers to the second to sixth questions referred in Case C-411/10 do not require to be qualified in any respect so as to take account of Protocol No 30.

Costs

123 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1 The decision adopted by a member state on the basis of article 3(2) of Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the member state responsible for examining an asylum application lodged in one of the member states by a third-country national, whether to examine an asylum application which is not its responsibility according to the criteria laid down in Chapter III of that Regulation, implements European Union law for the purposes of article 6EU of the EU Treaty and/or article 51 of the Charter of Fundamental Rights of the European Union.

2 European Union law precludes the application of a conclusive presumption that the member state which article 3(1) of Regulation No 343/2003 indicates as responsible observes the fundamental rights of the European Union. Article 4 of the Charter of Fundamental Rights of the European Union must be interpreted as meaning that the member states, including the national courts, may not transfer an asylum seeker to the "member state responsible" within the meaning of Regulation No 343/2003 where they cannot be unaware that systemic deficiencies in the asylum procedure and in the reception conditions of asylum seekers in that member state amount to substantial grounds for believing that the asylum seeker would face a real risk of being subjected to inhuman or degrading treatment within the meaning of that provision. Subject to the right itself to examine the application referred to in article 3(2) of Regulation No 343/2003, the finding that it is impossible to transfer an applicant to

another member state, where that state is identified as the member state responsible in accordance with the criteria set out in Chapter III of that Regulation, entails that the member state which should carry out that transfer must continue to examine the criteria set out in that Chapter in order to establish whether one of the following criteria enables another member state to be identified as responsible for the examination of the asylum application. The member state in which the asylum seeker is present must ensure that it does not worsen a situation where the fundamental rights of that applicant have been infringed by using a procedure for determining the member state responsible which takes an unreasonable length of time. If necessary, the first mentioned member state must itself examine the application in accordance with the procedure laid down in article 3(2) of Regulation No 343/2003.

3 Articles 1, 18 and 47 of the Charter of Fundamental Rights of the European Union do not lead to a different answer.

4 In so far as the preceding questions arise in respect of the obligations of the United Kingdom of Great Britain and Northern Ireland, the answers to the second to sixth questions referred in Case C-411/10 do not require to be qualified in any respect so as to take account of Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and the United Kingdom.

JESSICA GILES, Solicitor

10

JUDGMENT OF THE COURT (Grand Chamber)

8 April 2014 (*)

(Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union)

In Joined Cases C-293/12 and C-594/12,

REQUESTS for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria), made by decisions of 27 January and 28 November 2012, respectively, received at the Court on 11 June and 19 December 2012, in the proceedings

Digital Rights Ireland Ltd (C-293/12)

v

Minister for Communications, Marine and Natural Resources,

Minister for Justice, Equality and Law Reform,

Commissioner of the Garda Síochána,

Ireland,

The Attorney General,

intervener:

Irish Human Rights Commission,

and

Kärntner Landesregierung (C-594/12),

Michael Seitlinger,

Christof Tschohl and others,

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), E. Juhász, A. Borg Barthet, C.G. Fernlund and J.L. da Cruz Vilaça, Presidents of Chambers, A. Rosas, G. Arestis, J.-C. Bonichot, A. Arabadjiev, C. Toader and C. Vajda, Judges,

Advocate General: P. Cruz Villalón,

Registrar: K. Malacek, Administrator,

having regard to the written procedure and further to the hearing on 9 July 2013,

after considering the observations submitted on behalf of:

- Digital Rights Ireland Ltd, by F. Callanan, Senior Counsel, and F. Crehan, Barrister-at-Law, instructed by S. McGarr, Solicitor,
- Mr Seitlinger, by G. Otto, Rechtsanwalt,
- Mr Tschohl and Others, by E. Scheucher, Rechtsanwalt,
- the Irish Human Rights Commission, by P. Dillon Malone, Barrister-at-Law, instructed by S. Lucey, Solicitor,
- Ireland, by E. Creedon and D. McGuinness, acting as Agents, assisted by E. Regan, Senior Counsel, and D. Fennelly, Barrister-at-Law,
- the Austrian Government, by G. Hesse and G. Kunnert, acting as Agents,
- the Spanish Government, by N. Díaz Abad, acting as Agent,
- the French Government, by G. de Bergues and D. Colas and by B. Beaupère-Manokha, acting as Agents,
- the Italian Government, by G. Palmieri, acting as Agent, assisted by A. De Stefano, avvocato dello Stato,
- the Polish Government, by B. Majczyna and M. Szpunar, acting as Agents,
- the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,
- the United Kingdom Government, by L. Christie, acting as Agent, assisted by S. Lee, Barrister,
- the European Parliament, by U. Rösslein and A. Caiola and by K. Zejdová, acting as Agents,
- the Council of the European Union, by J. Monteiro and E. Sitbon and by I. Šulce, acting as Agents,
- the European Commission, by D. Maidani, B. Martenczuk and M. Wilderspin, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 12 December 2013,

gives the following

Judgment

1 These requests for a preliminary ruling concern the validity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic

communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

2 The request made by the High Court (Case C-293/12) concerns proceedings between (i) Digital Rights Ireland Ltd. ('Digital Rights') and (ii) the Minister for Communications, Marine and Natural Resources, the Minister for Justice, Equality and Law Reform, the Commissioner of the Garda Síochána, Ireland and the Attorney General, regarding the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications.

3 The request made by the Verfassungsgerichtshof (Constitutional Court) (Case C-594/12) concerns constitutional actions brought before that court by the Kärntner Landesregierung (Government of the Province of Carinthia) and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants regarding the compatibility with the Federal Constitutional Law (Bundes-Verfassungsgesetz) of the law transposing Directive 2006/24 into Austrian national law.

Legal context

Directive 95/46/EC

4 The object of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), according to Article 1 (1) thereof, is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with regard to the processing of personal data.

5 As regards the security of processing such data, Article 17(1) of that directive provides:

'Member States shall provide that the controller must implement appropriate technical and organi[s]ational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.'

Directive 2002/58/EC

6 The aim of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11, 'Directive 2002/58), according to Article 1(1) thereof, is to harmonise the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and to confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the European Union. According to Article 1(2), the provisions of that directive particularise and complement Directive 95/46 for the purposes mentioned in Article 1(1).

7 As regards the security of data processing, Article 4 of Directive 2002/58 provides:

'1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

– ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,

– protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,

– ensure the implementation of a security policy with respect to the processing of personal data,

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.'

8 As regards the confidentiality of the communications and of the traffic data, Article 5(1) and (3) of that directive provide:

'1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

...

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an

information society service explicitly requested by the subscriber or user to provide the service.'

9 Article 6(1) of Directive 2002/58 states:

'Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).'

10 Article 15 of Directive 2002/58 states in paragraph 1:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.'

Directive 2006/24

11 After having launched a consultation with representatives of law enforcement authorities, the electronic communications industry and data protection experts, on 21 September 2005 the Commission presented an impact assessment of policy options in relation to the rules on the retention of traffic data ('the impact assessment'). That assessment served as the basis for the drawing up of the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final, 'the proposal for a directive'), also presented on 21 September 2005, which led to the adoption of Directive 2006/24 on the basis of Article 95 EC.

12 Recital 4 in the preamble to Directive 2006/24 states:

'Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.'

13 According to the first sentence of recital 5 in the preamble to Directive 2006/24, '[s]everal Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences'.

14 Recitals 7 to 11 in the preamble to Directive 2006/24 read as follows:

'(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) [signed in Rome on 4 November 1950], everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive.
...

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.'

15 Recitals 16, 21 and 22 in the preamble to Directive 2006/24 state:

'(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.

(21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.'

16 Directive 2006/24 lays down the obligation on the providers of publicly available electronic communications services or of public communications networks to retain certain data which are generated or processed by them. In that context, Articles 1 to 9, 11 and 13 of the directive state:

'Article 1

Subject matter and scope

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2

Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) ..., and in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive:

(a) "data" means traffic data and location data and the related data necessary to identify the subscriber or user;

(b) "user" means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

(c) "telephone service" means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

(d) "user ID" means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;

(e) "cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated;

(f) "unsuccessful call attempt" means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3

Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4

Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of EU law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9

Supervisory authority

1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

...

Article 11

Amendment of Directive 2002/58/EC

The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

"1a. Paragraph 1 shall not apply to data specifically required by [Directive 2006/24/EC] to be retained for the purposes referred to in Article 1(1) of that Directive."

...

Article 13

Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties,

including administrative or criminal penalties, that are effective, proportionate and dissuasive.'

The actions in the main proceedings and the questions referred for a preliminary ruling

Case C-293/12

17 On 11 August 2006, Digital Rights brought an action before the High Court in which it claimed that it owned a mobile phone which had been registered on 3 June 2006 and that it had used that mobile phone since that date. It challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications and asked the national court, in particular, to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which requires telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State.

18 The High Court, considering that it was not able to resolve the questions raised relating to national law unless the validity of Directive 2006/24 had first been examined, decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. Is the restriction on the rights of the [p]laintiff in respect of its use of mobile telephony arising from the requirements of Articles 3, 4 ... and 6 of Directive 2006/24/EC incompatible with [Article 5(4)] TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims of:

(a) Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime?

and/or

b) Ensuring the proper functioning of the internal market of the European Union?

2. Specifically,

(i) Is Directive 2006/24 compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TFEU?

(ii) Is Directive 2006/24 compatible with the right to privacy laid down in Article 7 of the [Charter of Fundamental Rights of the European Union ("the Charter")] and Article 8 ECHR?

(iii) Is Directive 2006/24 compatible with the right to the protection of personal data laid down in Article 8 of the Charter?

(iv) Is Directive 2006/24 compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?

(v) Is Directive 2006/24 compatible with the right to [g]ood [a]dministration laid down in Article 41 of the Charter?

3. To what extent do the Treaties — and specifically the principle of loyal cooperation laid down in [Article 4(3) TEU] — require a national court to inquire into, and assess,

the compatibility of the national implementing measures for [Directive 2006/24] with the protections afforded by the [Charter], including Article 7 thereof (as informed by Article 8 of the ECHR)?'

Case C-594/12

19 The origin of the request for a preliminary ruling in Case C-594/12 lies in several actions brought before the Verfassungsgerichtshof by the Kärntner Landesregierung and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants, respectively, seeking the annulment of Paragraph 102a of the 2003 Law on telecommunications (Telekommunikationsgesetz 2003), which was inserted into that 2003 Law by the federal law amending it (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl I, 27/2011) for the purpose of transposing Directive 2006/24 into Austrian national law. They take the view, inter alia, that Article 102a of the Telekommunikationsgesetz 2003 infringes the fundamental right of individuals to the protection of their data.

20 The Verfassungsgerichtshof wonders, in particular, whether Directive 2006/24 is compatible with the Charter in so far as it allows the storing of many types of data in relation to an unlimited number of persons for a long time. The Verfassungsgerichtshof takes the view that the retention of data affects almost exclusively persons whose conduct in no way justifies the retention of data relating to them. Those persons are exposed to a greater risk that authorities will investigate the data relating to them, become acquainted with the content of those data, find out about their private lives and use those data for multiple purposes, having regard in particular to the unquantifiable number of persons having access to the data for a minimum period of six months. According to the referring court, there are doubts as to whether that directive is able to achieve the objectives which it pursues and as to the proportionality of the interference with the fundamental rights concerned.

21 In those circumstances the Verfassungsgerichtshof decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. Concerning the validity of acts of institutions of the European Union:

Are Articles 3 to 9 of [Directive 2006/24] compatible with Articles 7, 8 and 11 of the [Charter]?

2. Concerning the interpretation of the Treaties:

(a) In the light of the explanations relating to Article 8 of the Charter, which, according to Article 52(7) of the Charter, were drawn up as a way of providing guidance in the interpretation of the Charter and to which regard must be given by the Verfassungsgerichtshof, must [Directive 95/46] and Regulation (EC) No 45/2001 of the European Parliament and of the Council [of 18 December 2000] on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [OJ 2001 L 8, p. 1] be taken into account, for the purposes of assessing the permissibility of interference, as being of equal standing to the conditions under Article 8(2) and Article 52(1) of the Charter?

(b) What is the relationship between "Union law", as referred to in the final sentence of Article 52(3) of the Charter, and the directives in the field of the law on data protection?

(c) In view of the fact that [Directive 95/26] and Regulation ... No 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments resulting from subsequent secondary law be taken into account for the purpose of interpreting Article 8 of the Charter?

(d) Having regard to Article 52(4) of the Charter, does it follow from the principle of the preservation of higher levels of protection in Article 53 of the Charter that the limits applicable under the Charter in relation to permissible restrictions must be more narrowly circumscribed by secondary law?

(e) Having regard to Article 52(3) of the Charter, the fifth paragraph in the preamble thereto and the explanations in relation to Article 7 of the Charter, according to which the rights guaranteed in that article correspond to those guaranteed by Article 8 of the [ECHR], can assistance be derived from the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of that latter article?'

22 By decision of the President of the Court of 11 June 2013, Cases C-293/12 and C-594/12 were joined for the purposes of the oral procedure and the judgment.

Consideration of the questions referred

The second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12

23 By the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12, which should be examined together, the referring courts are essentially asking the Court to examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter.

The relevance of Articles 7, 8 and 11 of the Charter with regard to the question of the validity of Directive 2006/24

24 It follows from Article 1 and recitals 4, 5, 7 to 11, 21 and 22 of Directive 2006/24 that the main objective of that directive is to harmonise Member States' provisions concerning the retention, by providers of publicly available electronic communications services or of public communications networks, of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism, in compliance with the rights laid down in Articles 7 and 8 of the Charter.

25 The obligation, under Article 3 of Directive 2006/24, on providers of publicly available electronic communications services or of public communications networks to retain the data listed in Article 5 of the directive for the purpose of making them accessible, if necessary, to the competent national authorities raises questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11 of the Charter.

26 In that regard, it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain,

pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

27 Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

28 In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.

29 The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article (Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 47).

30 Whereas the references for a preliminary ruling in the present cases raise, in particular, the question of principle as to whether or not, in the light of Article 7 of the Charter, the data of subscribers and registered users may be retained, they also concern the question of principle as to whether Directive 2006/24 meets the requirements for the protection of personal data arising from Article 8 of the Charter.

31 In the light of the foregoing considerations, it is appropriate, for the purposes of answering the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12, to examine the validity of the directive in the light of Articles 7 and 8 of the Charter.

Interference with the rights laid down in Articles 7 and 8 of the Charter

32 By requiring the retention of the data listed in Article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24, as the Advocate General has pointed out, in particular, in paragraphs 39 and 40 of his Opinion, derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where

they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary.

33 To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that effect, Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 75).

34 As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.

35 Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R., *Leander v. Sweden*, 26 March 1987, § 48, Series A no 116; *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI). Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.

36 Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.

37 It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

Justification of the interference with the rights guaranteed by Articles 7 and 8 of the Charter

38 Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

39 So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.

40 Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without

prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.

41 As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.

42 It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest (see, to that effect, Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission* EU:C:2008:461, paragraph 363, and Cases C-539/10 P and C-550/10 P *Al-Aqsa* v *Council* EU:C:2012:711, paragraph 130). The same is true of the fight against serious crime in order to ensure public security (see, to that effect, Case C-145/09 *Tsakouridis* EU:C:2010:708, paragraphs 46 and 47). Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.

43 In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.

44 It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.

45 In those circumstances, it is necessary to verify the proportionality of the interference found to exist.

46 In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (see, to that effect, Case C-343/09 *Afton Chemical* EU:C:2010:419, paragraph 45; *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 74; Cases C-581/10 and C-629/10 *Nelson and Others* EU:C:2012:657, paragraph 71; Case C-283/11 *Sky Österreich* EU:C:2013:28, paragraph 50; and Case C-101/12 *Schaible* EU:C:2013:661, paragraph 29).

47 With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8

of the ECHR, Eur. Court H.R., *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).

48 In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

49 As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

50 That assessment cannot be called into question by the fact relied upon in particular by Mr Tschohl and Mr Seitlinger and by the Portuguese Government in their written observations submitted to the Court that there are several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication. Whilst, admittedly, that fact is such as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate, as the Advocate General has pointed out in paragraph 137 of his Opinion.

51 As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

52 So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 *IPI* EU:C:2013:715, paragraph 39 and the case-law cited).

53 In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.

54 Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, § 62 and 63; *Rotaru v. Romania*, § 57 to 59, and *S. and Marper v. the United Kingdom*, § 99).

55 The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, *S. and*

Marper v. the United Kingdom, § 103, and *M. K. v. France*, 18 April 2013, no. 19522/09, § 35).

56 As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

57 In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

58 Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

59 Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

60 Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

61 Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

62 In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

63 Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

64 Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

65 It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

66 Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

67 Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

68 In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two

previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 *Commission* v *Austria* EU:C:2012:631, paragraph 37).

69 Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.

70 In those circumstances, there is no need to examine the validity of Directive 2006/24 in the light of Article 11 of the Charter.

71 Consequently, the answer to the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12 is that Directive 2006/24 is invalid.

The first question and the second question, parts (a) and (e), and the third question in Case C-293/12 and the second question in Case C-594/12

72 It follows from what was held in the previous paragraph that there is no need to answer the first question, the second question, parts (a) and (e), and the third question in Case C-293/12 or the second question in Case C-594/12.

Costs

73 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national courts, the decision on costs is a matter for those courts. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid.

[Signatures]

---

* Languages of the case: English and German.